Cyber Security

Introduction

The project is now properly running in the PLC (or Simulator). This chapter explains how to make sure that someone will not disrupt its normal functioning via a Cyber Attack; such as Stuxnet?

The M580 is one of the first PLC with enabled security features that make it a harder target for cyber attacks.

This exercise explains how to enable these features and how they will affect the architecture.

Further Training:

1) To make the system even more secure; refer to the cyber security topic in the second chapter.

2) The Schneider Electric document; *Cyber Security for Automation Systems(Unity Pro v8.0)*

Topic Objectives

By the end of this chapter the student will be able to:

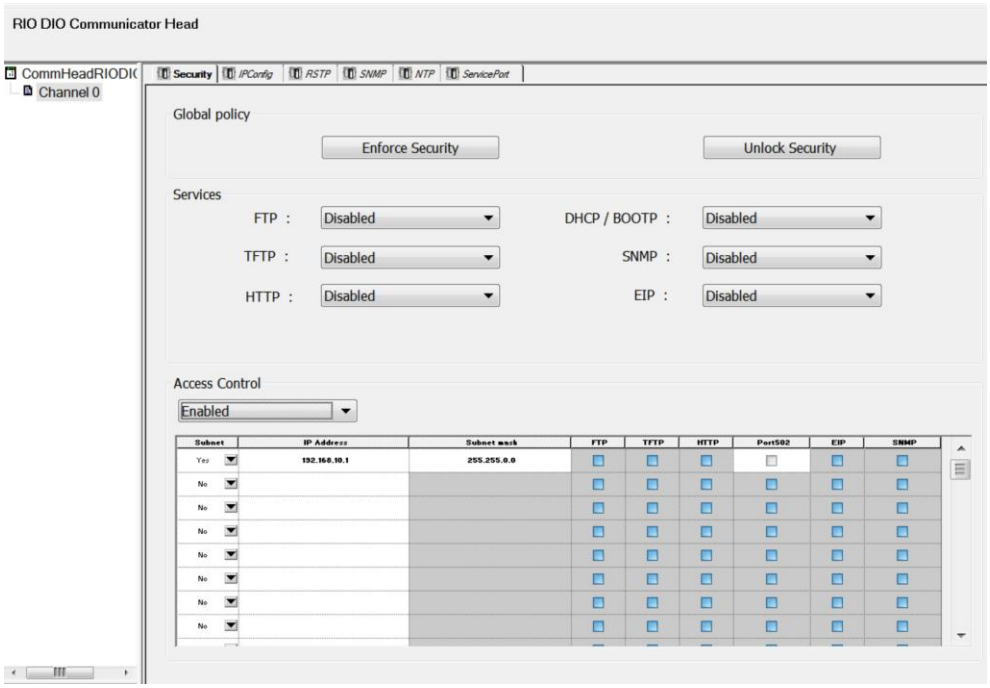
- Identify Cyber Security measures within the M580.
- Deploy Cyber Security measures in M580 architecture.

Cyber Security (cont.)

Securing Services

Along with the Achilles Level 2 implementation, a key feature of the M580 is the ability to prevent certain Ethernet based services from running.

The majority of settings are located on the CPU Embedded Ethernet port **Security** tab:



Hints & Tips

The Schneider Electric recommendation is to **disable** all unused Services.

Cyber Security (cont.)

Restricting Connection to Some Devices

From this tab the student can also decide which IP addresses are allowed/not allowed to communicate with the M580.

Restricting access to some IP addresses makes hacking much more difficult.

Summary of the M580's Security Tab

This table explains the functionality of the settings on the **Security** tab:

FTP	Default value: **Disabled** Schneider Electric recommends disabling this service when not in use. This setting disables: - firmware upgrade - SD memory card data storage - device configuration management using the FDR service
TFTP	Default value: **Disabled** Schneider Electric recommends disabling this service when not in use. This setting disables: - the ability to read RIO drop configurations - the ability to manage device configurations using the FDR service
HTTP	Default value: **Disabled** Schneider Electric recommends disabling this service when not in use. This setting disables Web access.
Achilles level 2	Default value: **Enabled** - Setting the feature to Enabled increases Ethernet frame filtering to improve the level of security and robustness. - Setting the feature to Disabled increases system performance by reducing the Ethernet frame filtering capability.
Access Control	Default value: **Enabled** When Enabled, you can restrict access from specific devices to specific devices and define the devices that allow traffic only.
Enforce Security	Click to set: - FTP, TFTP, and HTTP to Disabled - Achilles level 2 and Access Control to Enabled
Unlock Security	Click to set: - FTP, TFTP, and HTTP to Enabled - Achilles level 2 and Access Control to Disabled
Authorized addresses	Enter the addresses that you want the system to authorize: - IP Address: 0.0.0.0 ... 255.255.255.255 - Subnet: Yes / No - Subnet mask: 0.0.0.0 ... 255.255.255.255 NOTE: This field can be edited when **Access Control** is set to **Disabled**.

Cyber Security (cont.)

Note:
1) Be very careful when activating the security features, especially IP restriction because the PLC can become inaccessible: by IP, SD card and USB! In that case the PLC is useless. Thus be careful experimenting with these features at the same time.

2) It is advised that all protocols are disabled and Achilles 2 Cyber Security is enabled when a project is started. Unity Pro will then request protocols to be activated when they are required. Only the features the project requires are therefore enabled, which improves Cyber Security. Once the configuration is working access to specific IP addresses can then also be restricted.

Cyber Secured NOC

Quite often NOCs are connected to a SCADA system, making them indirectly connected to an internet network and away from cyber attacks.

Note:
To avoid intrusion from the NOC a new secured NOC module will be released soon. It will include Cyber Security features similar to the ones of the M580.

Exercise – Cyber Security

Learning Outcomes

By the completion of this exercise the student will:

- Activate the Achilles level 2 feature
- Enable/disable services

Equipment Required

To complete this exercise on a PLC the student will need

- One M580 PLC (any CPU)
- A BMX or BME rack
- A compatible power supply
- A micro USB cable or an RJ45 cable

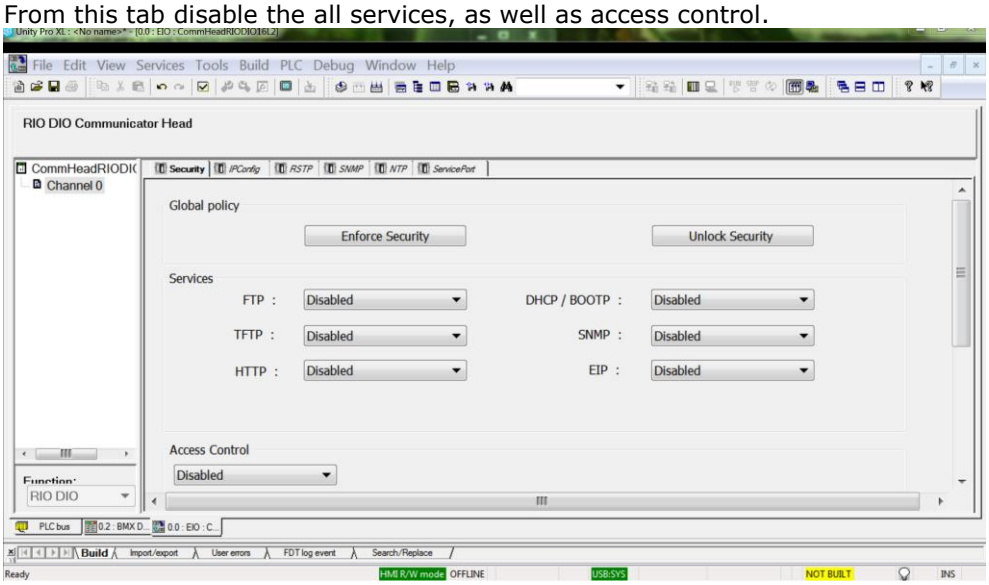
Modify the cyber security settings.

i. Open the main rack configuration window.

ii. Double click the **M580 ports**; making sure to not click the **PLC**.

iii. From the newly opened window, click the **Security** tab.

iv. From this tab disable the all services, as well as access control.



v. Relevant services will now be activated for each exercise.