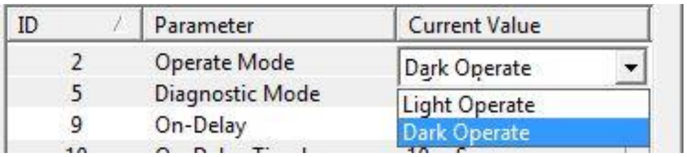
Modify Sensor Data

Scenario One:

If using a network Sensor change the Operate Mode

This will cause the Sensor to work oppose as intended.

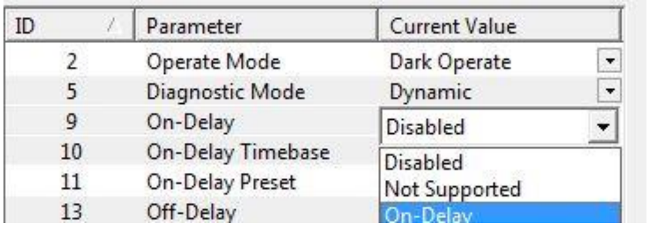


ID	Parameter	Current Value
2	Operate Mode	Dark Operate
5	Diagnostic Mode	
9	On-Delay	

Scenario Two:

Turn On / Off timing circuit in the Sensor

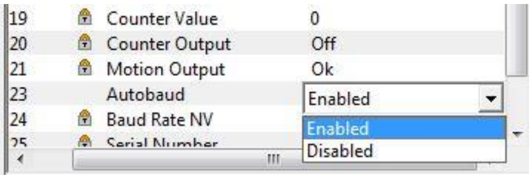
This will cause the Sensor signal to reach the PLC in a Longer / Shorter Time than intended



ID	Parameter	Current Value
2	Operate Mode	Dark Operate
5	Diagnostic Mode	Dynamic
9	On-Delay	Disabled
10	On-Delay Timebase	
11	On-Delay Preset	
13	Off-Delay	

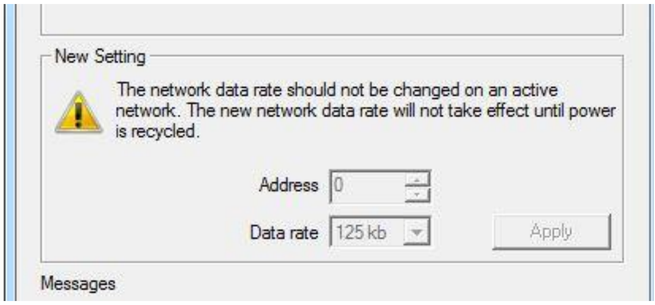
Scenario Three:

Change the Baud Rate Setting so the Sensor will no longer communicate on the network



19	Counter Value	0
20	Counter Output	Off
21	Motion Output	Ok
23	Autobaud	Enabled
24	Baud Rate NV	
25	Serial Number	

Change Baud Setting:



New Setting

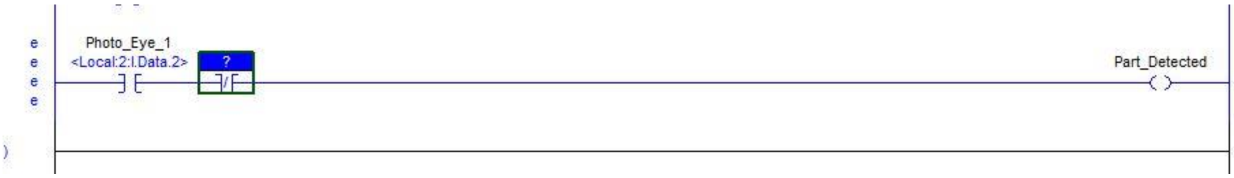
The network data rate should not be changed on an active network. The new network data rate will not take effect until power is recycled.

Address: 0

Data rate: 125 kb

Scenario Four:

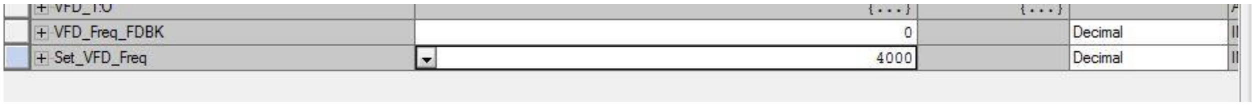
Change the Instruction in the PLC Project that monitors the Sensor



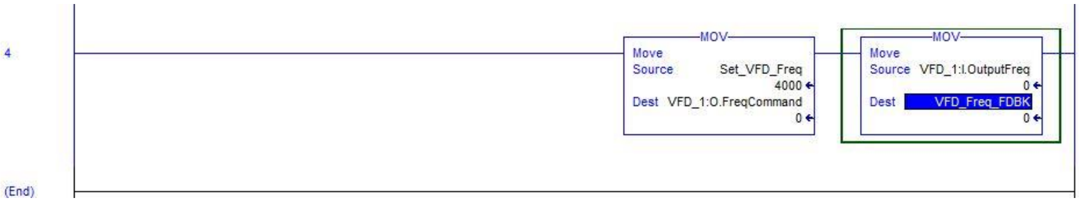
Attack PLC Register Values:

Scenario One:

Modify Tag values in the PLC so the PLC sending incorrect data to a device.

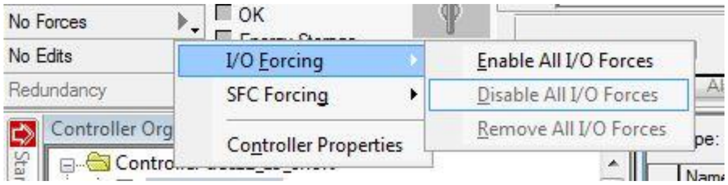


+ VFD_1:O	{...}	{...}	
+ VFD_Freq_FDBK	0		Decimal
+ Set_VFD_Freq	4000		Decimal



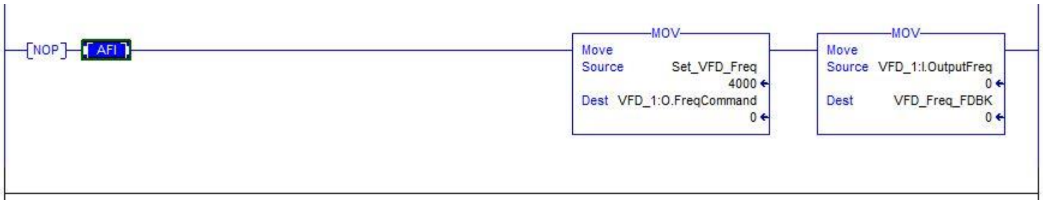
Scenario Two:

Force I/O values in the PLC so the values are overriding the PLC data.



Scenario Three:

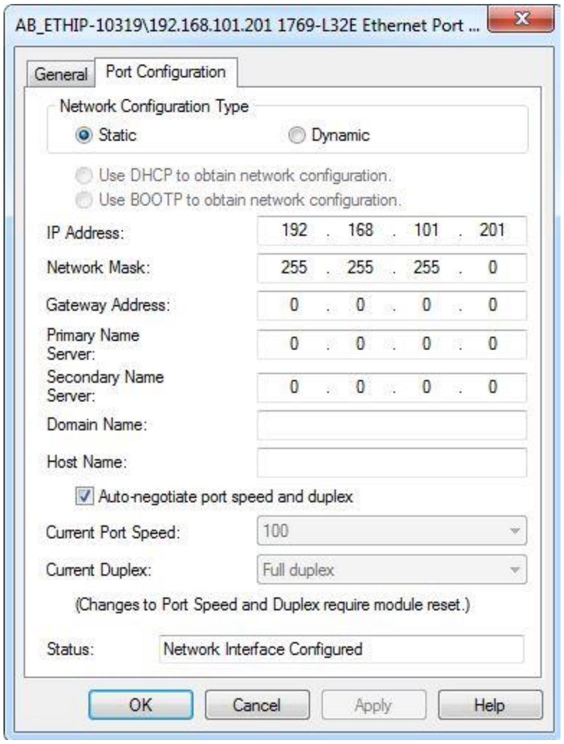
Modify instruction so PLC Register / Tag values are not sent to the intended device



Denial of Service against a PLC

Scenario One:

Change IP Addressing settings on Ethernet Modules



AB_ETHIP-10319\192.168.101.201 1769-L32E Ethernet Port ...

Network Configuration Type

● Static ○ Dynamic

○ Use DHCP to obtain network configuration.

○ Use BOOTP to obtain network configuration.

IP Address: 192 . 168 . 101 . 201

Network Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

Primary Name Server: 0 . 0 . 0 . 0

Secondary Name Server: 0 . 0 . 0 . 0

Domain Name:

Host Name:

☑ Auto-negotiate port speed and duplex

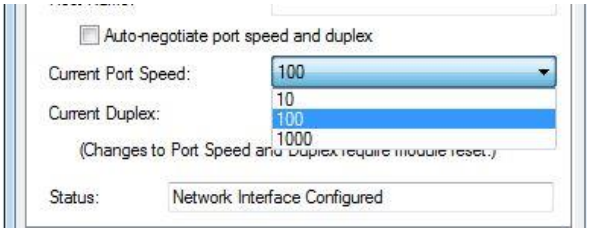
Current Port Speed: 100

Current Duplex: Full duplex

(Changes to Port Speed and Duplex require module reset.)

Status: Network Interface Configured

Change Speed and Duplex settings on the Communication Modules



□ Auto-negotiate port speed and duplex

Current Port Speed: 100

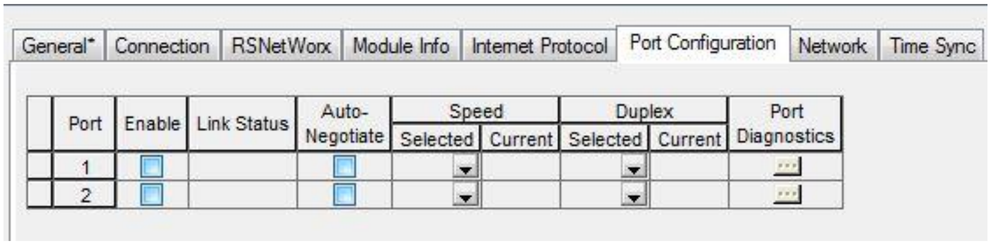
Current Duplex:

(Changes to Port Speed and Duplex require module reset.)

Status: Network Interface Configured

Scenario Two:

Disable Communication Ports on the Ethernet Modules

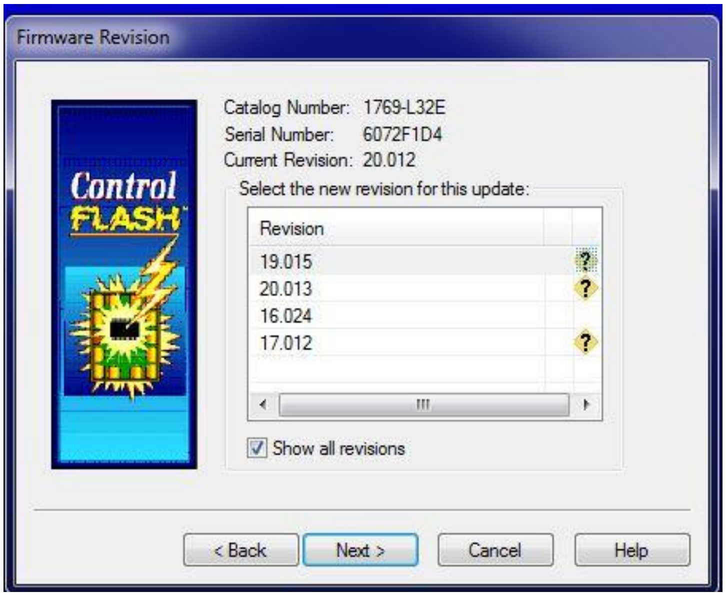


Port	Enable	Link Status	Auto-Negotiate	Speed		Duplex		Port Diagnostics
				Selected	Current	Selected	Current	
1	□		□					...
2	□		□					...

Scenario Three:

Change PLC firmware

This can prevent access to the PLC depending on software revision of application


Firmware Revision

Catalog Number: 1769-L32E
Serial Number: 6072F1D4
Current Revision: 20.012

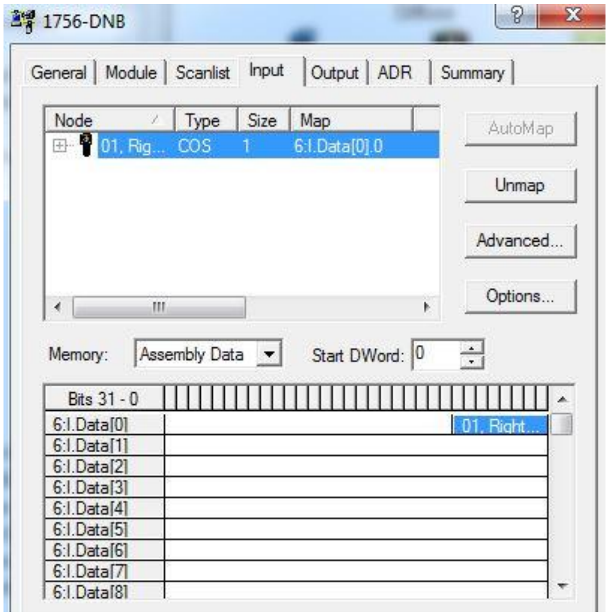
Select the new revision for this update:

Revision
19.015
20.013
16.024
17.012

☑ Show all revisions

Scenario Four:

Change I/O mapping setting in communication modules


1756-DNB

Node	Type	Size	Map
01, Rig...	COS	1	6:I.Data[0].0

Memory: Assembly Data
Start DWord: 0

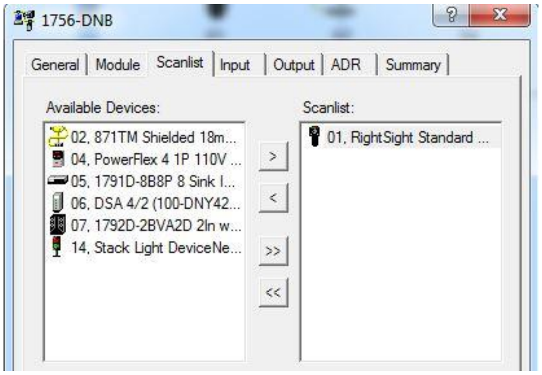
Bits 31 - 0	
6:I.Data[0]	01, Right...
6:I.Data[1]	
6:I.Data[2]	
6:I.Data[3]	
6:I.Data[4]	
6:I.Data[5]	
6:I.Data[6]	
6:I.Data[7]	
6:I.Data[8]	

Data flow between a device and a PLC will be incorrect.

Scenario Five:

Change Communication module Device setting.

This can prevent a PLC from accessing data from a device if not configured correctly.



Available Devices:

- 02, 871TM Shielded 18m...
- 04, PowerFlex 4 1P 110V ...
- 05, 1791D-8B8P 8 Sink I...
- 06, DSA 4/2 (100-DNY42...
- 07, 1792D-2BVA2D 2In w...
- 14, Stack Light DeviceNe...

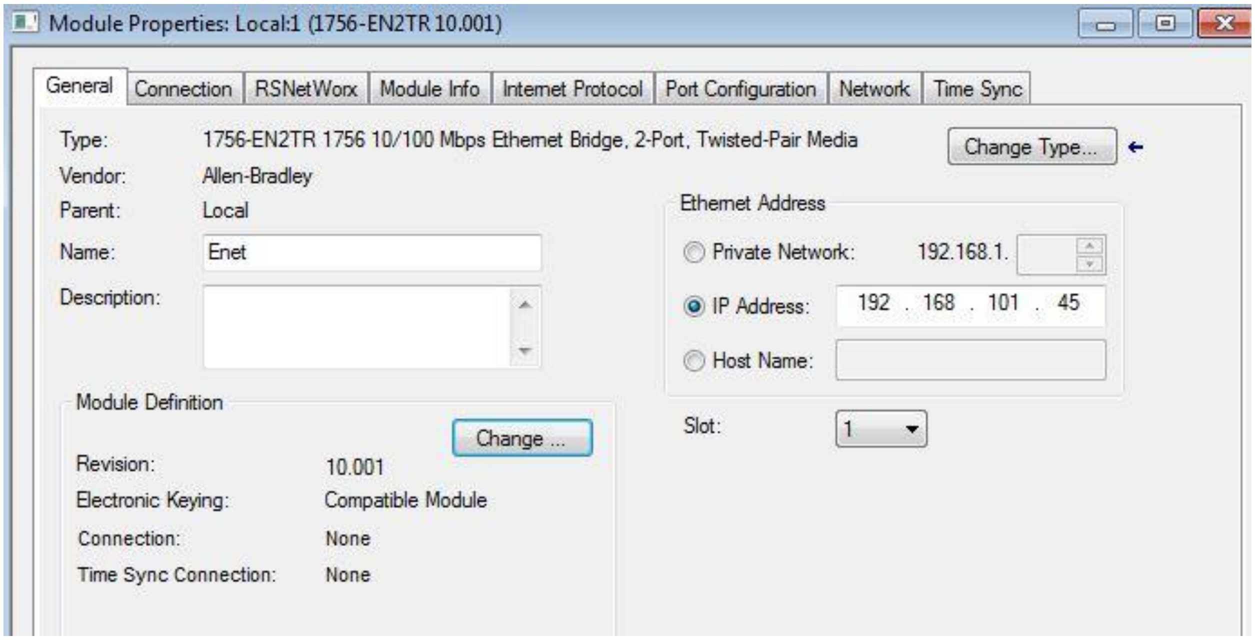
Scanlist:

- 01, RightSight Standard ...

Scenario Six:

Modify Property Settings in the PLC I/O Configuration

This will prevent the PLC from accessing the device.



Type: 1756-EN2TR 1756 10/100 Mbps Ethernet Bridge, 2-Port, Twisted-Pair Media

Vendor: Allen-Bradley

Parent: Local

Name: Enet

Description:

Module Definition

Revision: 10.001

Electronic Keying: Compatible Module

Connection: None

Time Sync Connection: None

Ethernet Address

○ Private Network: 192.168.1.

● IP Address: 192 . 168 . 101 . 45

○ Host Name:

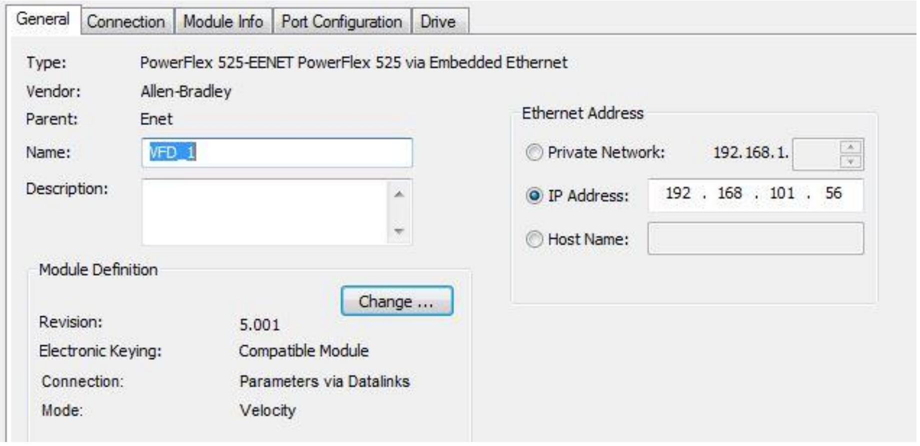
Slot: 1

Disable a Variable Frequency Drive

Scenario One:

Change VFD settings in the PLC’s configuration to prevent the PLC from accessing the VFD

Change the IP address.



Type: PowerFlex 525-EENET PowerFlex 525 via Embedded Ethernet

Vendor: Allen-Bradley

Parent: Enet

Name: VFD_1

Description:

Module Definition

Revision: 5.001

Electronic Keying: Compatible Module

Connection: Parameters via Datalinks

Mode: Velocity

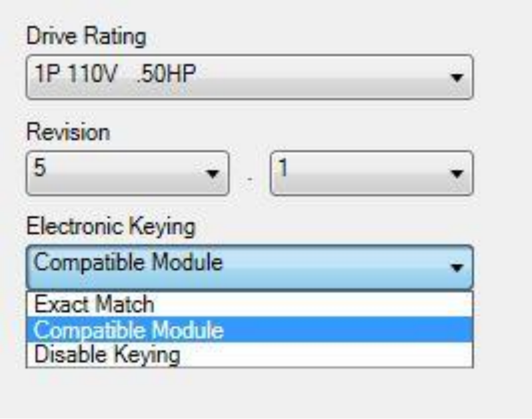
Ethernet Address

○ Private Network: 192.168.1.

● IP Address: 192 . 168 . 101 . 56

○ Host Name:

Change the Electronic Keying Information

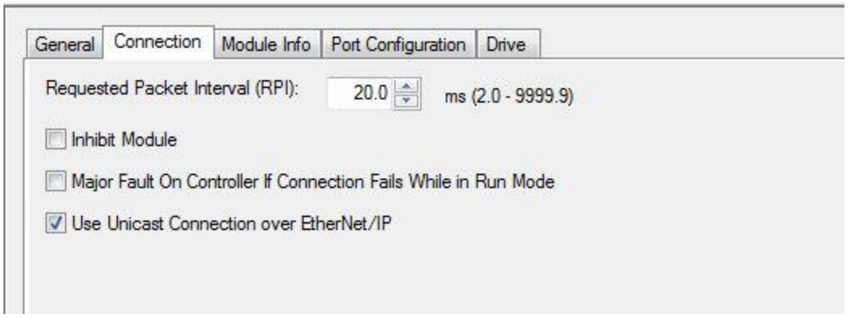


Drive Rating: 1P 110V .50HP

Revision: 5 . 1

Electronic Keying: Compatible Module

Change response to a configuration problem, i.e. fault the VFD



Requested Packet Interval (RPI): 20.0 ms (2.0 - 9999.9)

☐ Inhibit Module

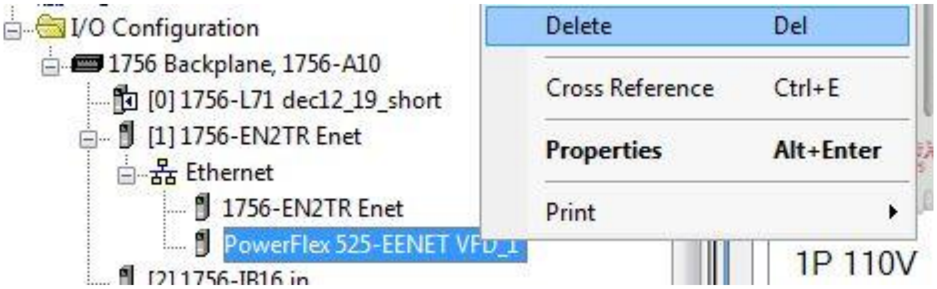
☐ Major Fault On Controller If Connection Fails While in Run Mode

☑ Use Unicast Connection over EtherNet/IP

Scenario Two:

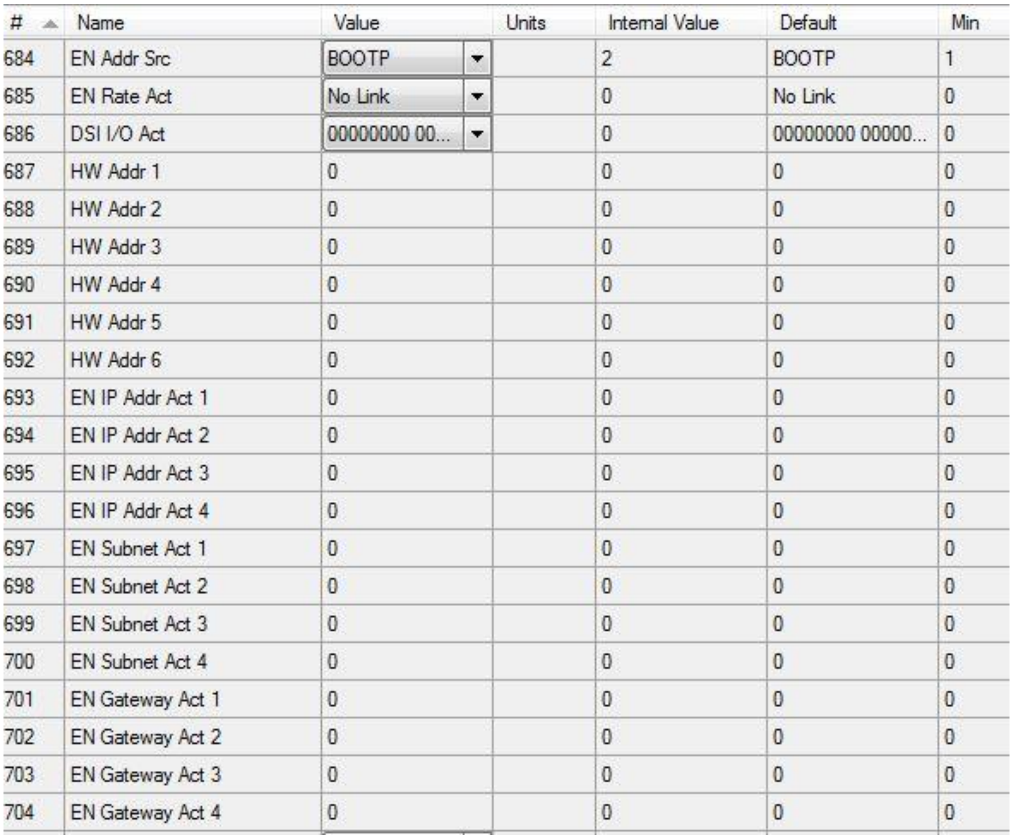
Delete the VFD from the PLC I/O configuration

The PLC and the will not communicate.



Scenario Three:

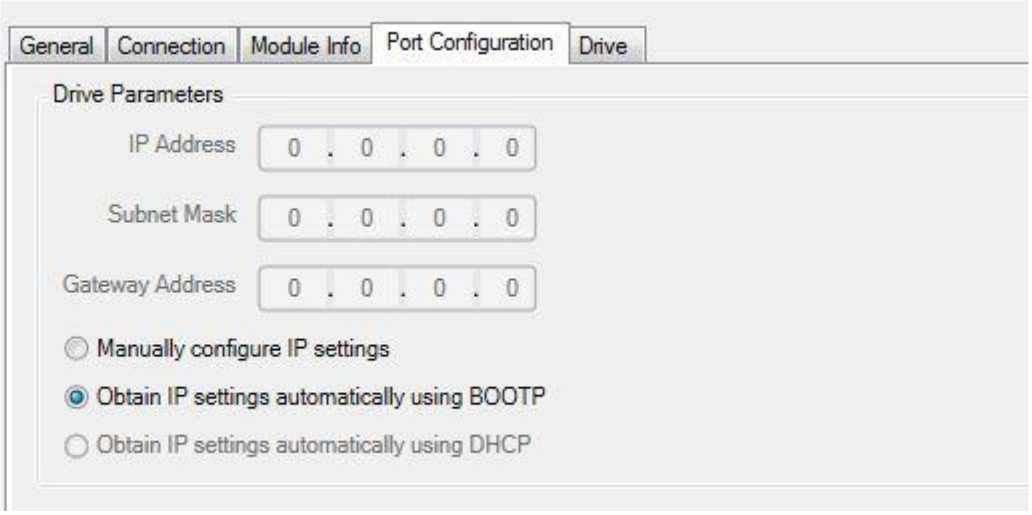
Change BOOTP parameter setting and / or Ethernet addressing settings in the VFD to prevent the PLC and VFD from communicating



#	Name	Value	Units	Internal Value	Default	Min
684	EN Addr Src	BOOTP		2	BOOTP	1
685	EN Rate Act	No Link		0	No Link	0
686	DSI I/O Act	00000000 00...		0	00000000 00000...	0
687	HW Addr 1	0		0	0	0
688	HW Addr 2	0		0	0	0
689	HW Addr 3	0		0	0	0
690	HW Addr 4	0		0	0	0
691	HW Addr 5	0		0	0	0
692	HW Addr 6	0		0	0	0
693	EN IP Addr Act 1	0		0	0	0
694	EN IP Addr Act 2	0		0	0	0
695	EN IP Addr Act 3	0		0	0	0
696	EN IP Addr Act 4	0		0	0	0
697	EN Subnet Act 1	0		0	0	0
698	EN Subnet Act 2	0		0	0	0
699	EN Subnet Act 3	0		0	0	0
700	EN Subnet Act 4	0		0	0	0
701	EN Gateway Act 1	0		0	0	0
702	EN Gateway Act 2	0		0	0	0
703	EN Gateway Act 3	0		0	0	0
704	EN Gateway Act 4	0		0	0	0

Scenario Four:

Change VFD port settings to disable communication between the PLC and VFD.



Drive Parameters

IP Address 0 . 0 . 0 . 0

Subnet Mask 0 . 0 . 0 . 0

Gateway Address 0 . 0 . 0 . 0

○ Manually configure IP settings

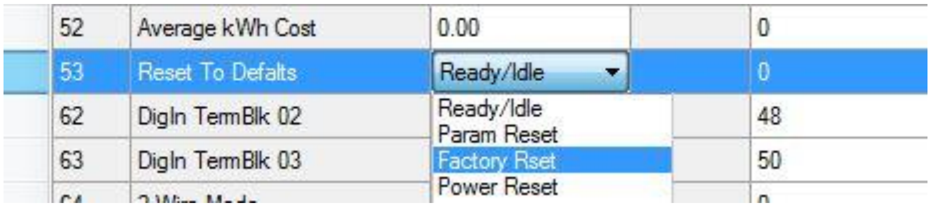
● Obtain IP settings automatically using BOOTP

○ Obtain IP settings automatically using DHCP

Scenario Five:

Reset the VFD parameters back to factory defaults.

This will cause the VFD to fault and change parameters.



52	Average kWh Cost	0.00		0
53	Reset To Defalts	Ready/Idle		0
62	DigIn TermBlk 02			48
63	DigIn TermBlk 03			50

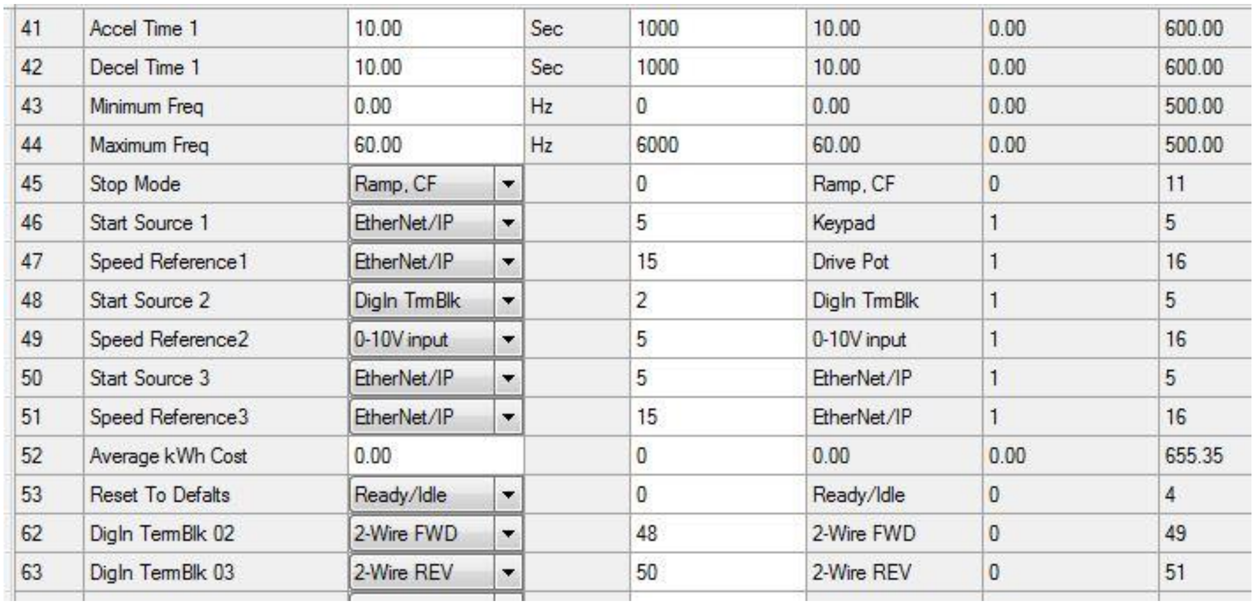
Scenario Six:

Change parameters so the VFD does not respond has intended.

There are a number of parameters that will cause complications

Some of the more common ones are shown on the next page.

- Accel / Decel – VFD response will be too fast or slow depending on settings
- Min / Max Freq – VFD will not run motor at intended speed.
- Stop Mode – VFD controls stopping of a motor
- Start Source – how the VFD gets a signal to run the motor
- Speed Reference – where the VFD is getting a signal to run the motor at a particular speed.



41	Accel Time 1	10.00	Sec	1000	10.00	0.00	600.00
42	Decel Time 1	10.00	Sec	1000	10.00	0.00	600.00
43	Minimum Freq	0.00	Hz	0	0.00	0.00	500.00
44	Maximum Freq	60.00	Hz	6000	60.00	0.00	500.00
45	Stop Mode	Ramp, CF		0	Ramp, CF	0	11
46	Start Source 1	EtherNet/IP		5	Keypad	1	5
47	Speed Reference1	EtherNet/IP		15	Drive Pot	1	16
48	Start Source 2	DigIn TrmBlk		2	DigIn TrmBlk	1	5
49	Speed Reference2	0-10V input		5	0-10V input	1	16
50	Start Source 3	EtherNet/IP		5	EtherNet/IP	1	5
51	Speed Reference3	EtherNet/IP		15	EtherNet/IP	1	16
52	Average kWh Cost	0.00		0	0.00	0.00	655.35
53	Reset To Defalts	Ready/Idle		0	Ready/Idle	0	4
62	DigIn TermBlk 02	2-Wire FWD		48	2-Wire FWD	0	49
63	DigIn TermBlk 03	2-Wire REV		50	2-Wire REV	0	51