How to Configure the MGate 5114 with IEC 60870-5-104 SCADA

Moxa Technical Support Team
support@moxa.com

Contents

 Released on January 03, 2019

About Moxa

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

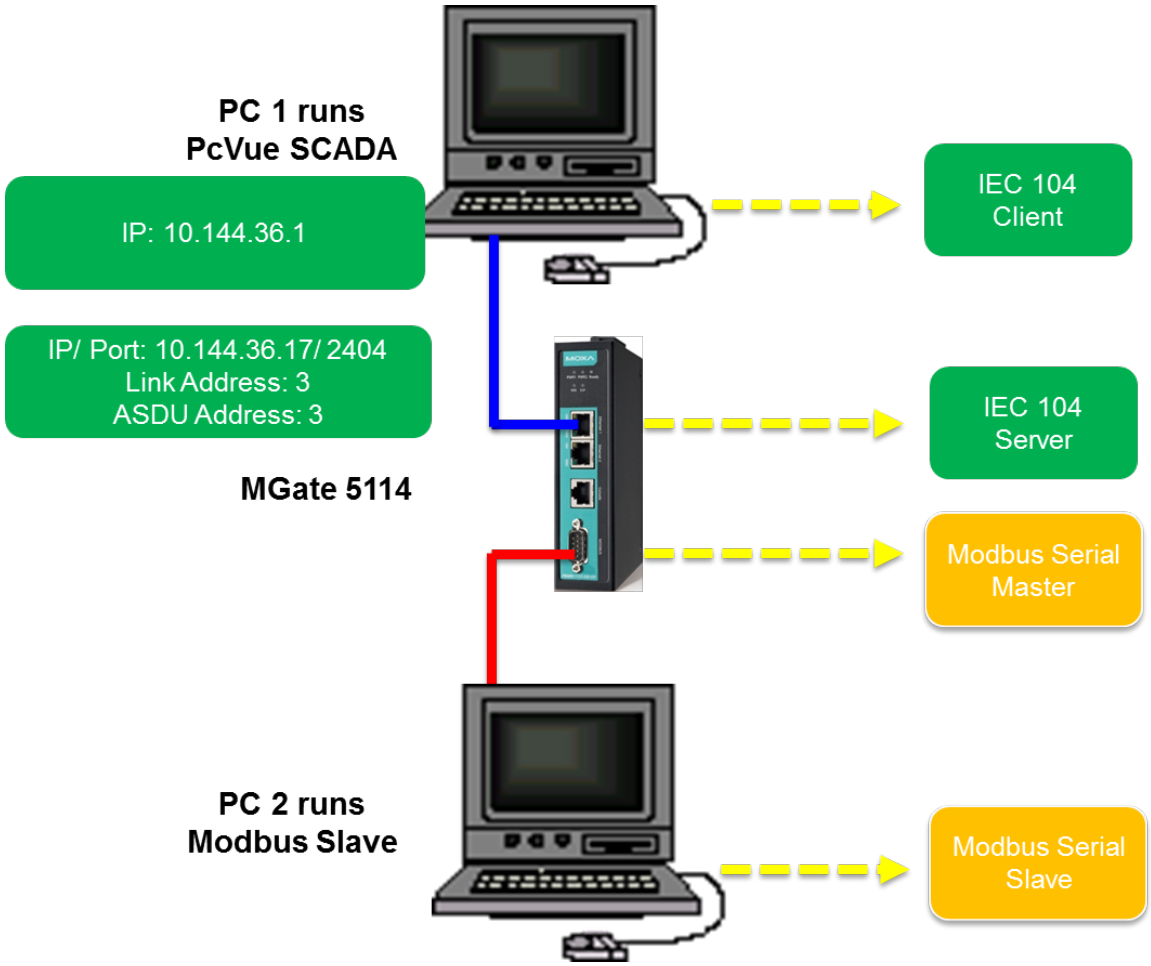
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

MOXA®
Reliable Networks ▲ Sincere Service

1 System Topology

This technical note demonstrates how to use the **MGate 5114** to communicate with **IEC 60870-5-104 SCADA**. We use **PcVue SCADA** as an IEC 60870-5-104 Client to monitor remote Modbus RTU via the MGate 5114. In this topology, it shows how the MGate 5114 converts between **IEC 60870-5-104 Client** and **Modbus RTU Slave**.

< System Topology >



2 Protocol Simulators

2.1 PcVue SCADA

PcVue SCADA system is published by **ARC Informatique**. We use Version **11.1** in this demo. It has an IEC 60870-5-104 built-in driver for IEC 60870-5-104 communication.

2.2 Modbus Slave

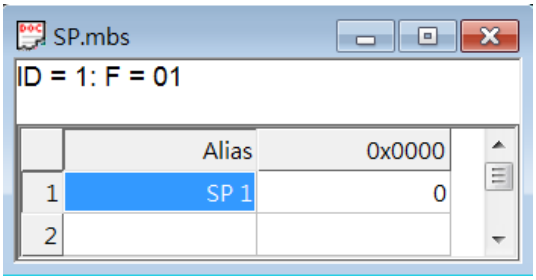
Modbus Slave is the very popular Modbus slave simulator for testing and debugging your Modbus devices. It supports Modbus RTU/ASCII and Modbus TCP/IP.

Download website: http://www.modbustools.com/download.html

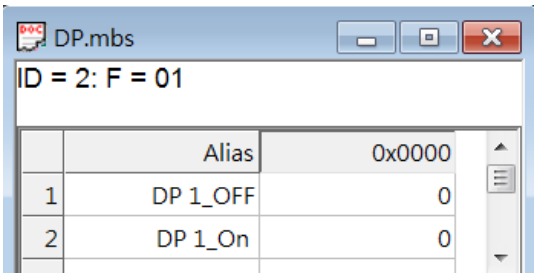
3 Simulation of Modbus Slave Settings

In the topology, PC2 runs **Modbus Slave** and connects to the MGate 5114's serial port.
The serial parameters are defined as: **115200, 8/N/1, RS-485 (2-wire)**
We simulate various Modbus devices with different slave IDs.

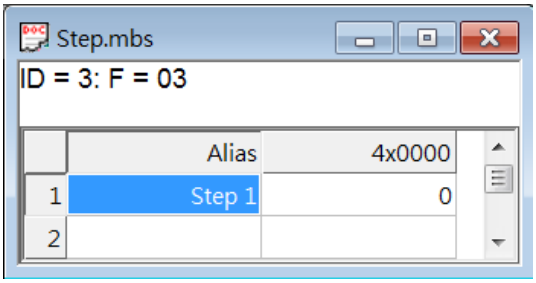
< SP Definition, Slave ID 1 >



< DP Definition, Slave ID 2 >

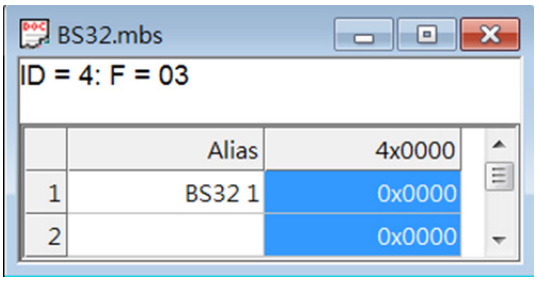


< Step Definition, Slave ID 3 >



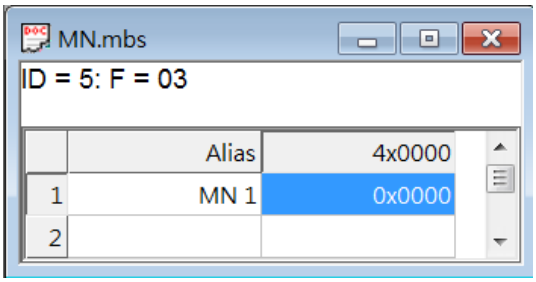
(Display: Signed)

< BS32 Definition, Slave ID 4 >



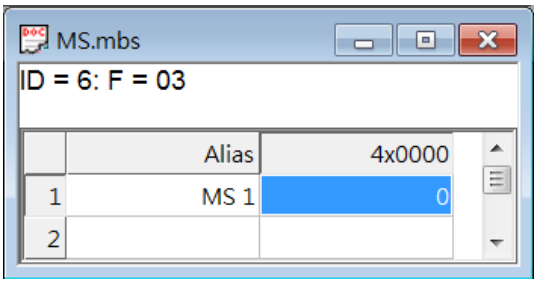
(Display: Hex)

< MN Definition, Slave ID 5 >



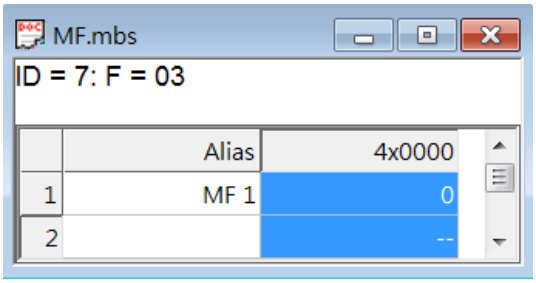
(Display: Hex)

< MS Definition, Slave ID 6 >



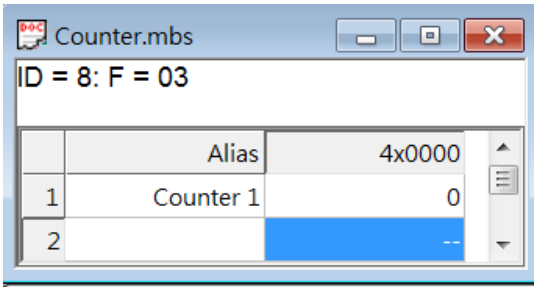
(Display: Signed)

< MF Definition, Slave ID 7 >



(Display: Float CD AB)

< Counter Definition, Slave ID 8 >



(Display: Long CD AB)

4 MGate 5114 Settings

For the MGate's 5114 settings, we should access the web console to configure. Here are the configuration steps:

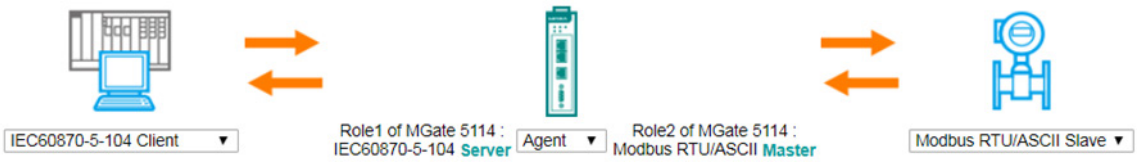
- Step 1. Configuration of serial parameters (Serial Settings)
- Step 2. Protocol selection (Protocol Conversion)
- Step 3. Configuration of protocol 1 (Modbus RTU Master Settings)
- Step 4. Configuration of protocol 2 (IEC 60870-5-104 Server Settings)
- Step 5. I/O data mapping

Step 1. Configuration of Serial Parameters (Serial Settings)

Go to **Serial Settings** to configure the serial parameters, which should be the same as your Modbus device. Here, we configure it as: **115200, 8/N/1, RS-485 (2-wire)**

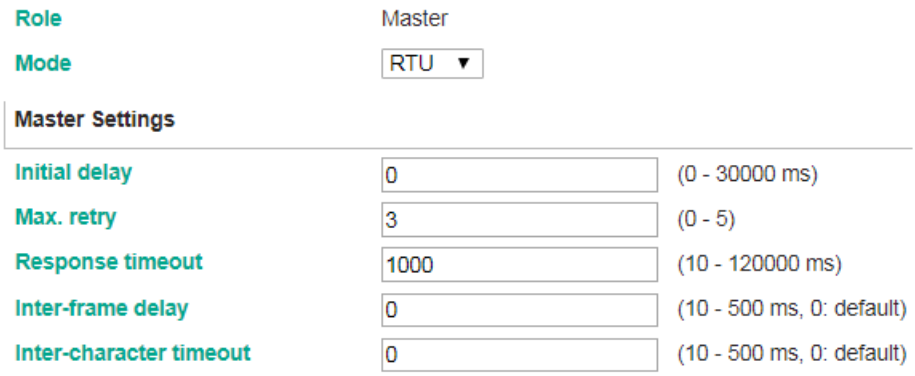
Step 2. Protocol Selection (Protocol Conversion)

For a protocol gateway, we have to configure each protocol's role that should be selected here. This is an example of converting from Modbus RTU to IEC 60870-5-104. After protocol selection, the next steps are to configure each side of the MGate.

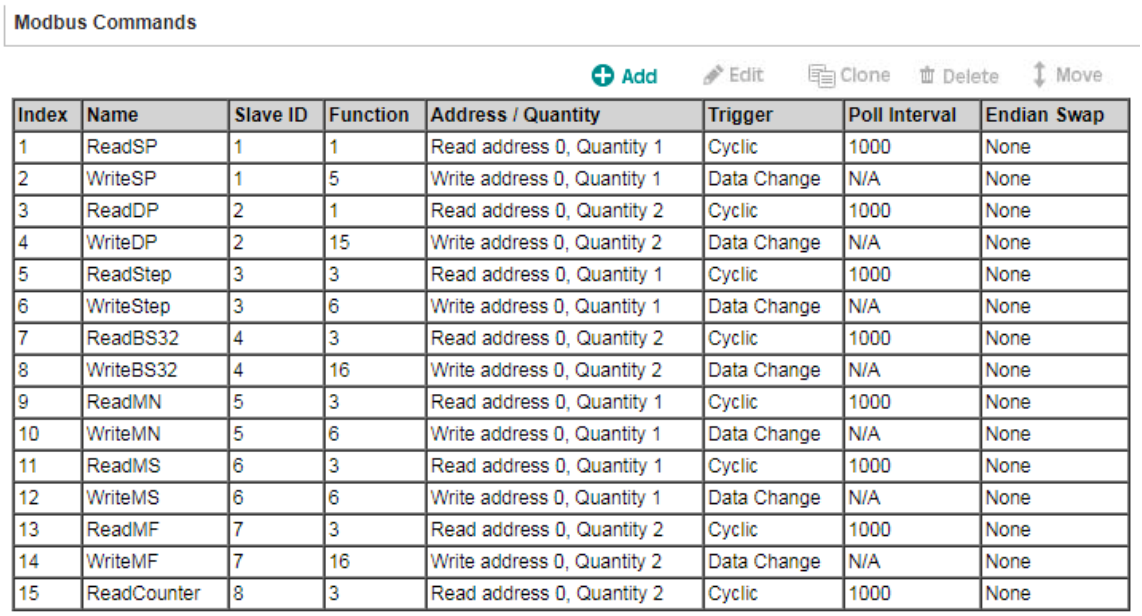


Step 3. Configuration of Protocol 1 (Modbus RTU Master Settings)

In Modbus RTU Master Settings, the related parameters can be configured. Here, we use the default settings. For details, you can refer to the user's manual.



Then, we have to monitor andcontrol the Modbus slave device. Therefore, Modbus commands should be configured. The Modbus commands are shown as below:



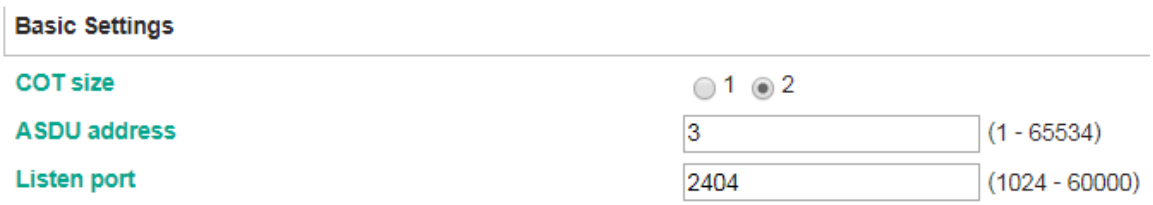
Index	Name	Slave ID	Function	Address / Quantity	Trigger	Poll Interval	Endian Swap
1	ReadSP	1	1	Read address 0, Quantity 1	Cyclic	1000	None
2	WriteSP	1	5	Write address 0, Quantity 1	Data Change	N/A	None
3	ReadDP	2	1	Read address 0, Quantity 2	Cyclic	1000	None
4	WriteDP	2	15	Write address 0, Quantity 2	Data Change	N/A	None
5	ReadStep	3	3	Read address 0, Quantity 1	Cyclic	1000	None
6	WriteStep	3	6	Write address 0, Quantity 1	Data Change	N/A	None
7	ReadBS32	4	3	Read address 0, Quantity 2	Cyclic	1000	None
8	WriteBS32	4	16	Write address 0, Quantity 2	Data Change	N/A	None
9	ReadMN	5	3	Read address 0, Quantity 1	Cyclic	1000	None
10	WriteMN	5	6	Write address 0, Quantity 1	Data Change	N/A	None
11	ReadMS	6	3	Read address 0, Quantity 1	Cyclic	1000	None
12	WriteMS	6	6	Write address 0, Quantity 1	Data Change	N/A	None
13	ReadMF	7	3	Read address 0, Quantity 2	Cyclic	1000	None
14	WriteMF	7	16	Write address 0, Quantity 2	Data Change	N/A	None
15	ReadCounter	8	3	Read address 0, Quantity 2	Cyclic	1000	None

Step 4. Configuration of Protocol 2 (IEC 60870-5-104 Server Settings)

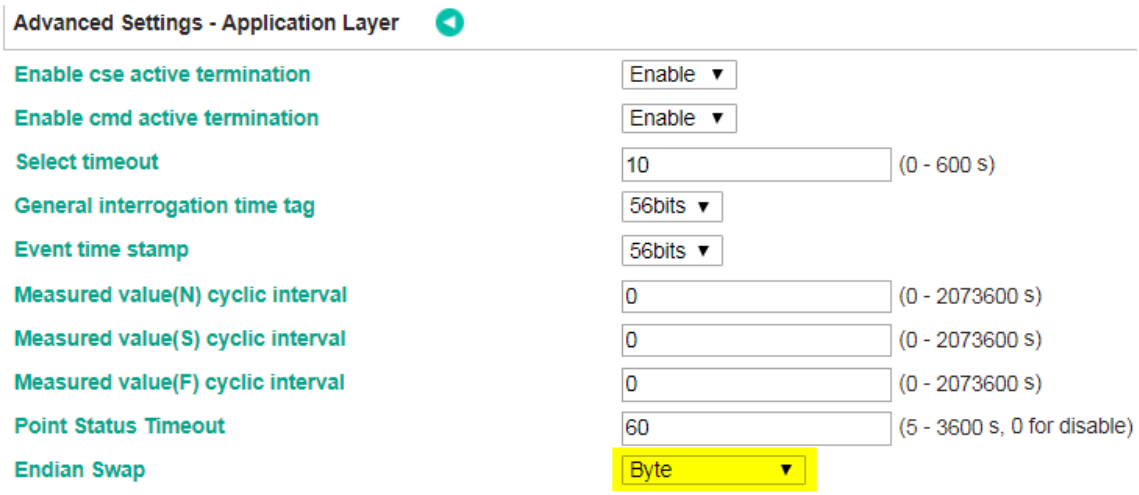
In **IEC 60870-5-104 Sever Settings**, there are **Basic Settings** and **Advanced Settings**.

For **Basic Settings**, we configure the parameters as below:

- COT size as "2"
- ASDU address as "3"
- Listen Port as **2404** port.



For **Advanced Settings**, we configure the parameters as below:



Note: If the data can't be read correctly, it may be caused by the big-endian/little-endian. You can try to adjust the **Endian Swap** parameters. The default value "Byte" is for most scenarios.

The Modbus RTU slave values need to be monitored or controlled by IEC 60870-5-104 Client. At this stage, we have to plan the data mapping table between IEC 60870-5-104 and Modbus RTU. The mapping table should show as below:

Mapping IEC 60870-5-104 Data Object	Modbus Data Type	Modbus Command	Points Mapping
Single Points	**Coil**	ReadSP, WriteSP	SP 1 → Coil 1
Double Points	**Coil**	ReadDP, WriteDP	DP 1 → Coil 1~2
Step position	**Register**	ReadStep, WriteStep	Step 1 → Register 1
Bitstring32	**Register**	ReadBS32, WriteBS32	BS32 1 → Register 1 and 2
Measure value(N)	**Register**	ReadMN, WriteMN	MN 1 → Register 1
Measure value(S)	**Register**	ReadMS, WriteMS	MS 1 → Register 1
Measure value(F)	**Register**	ReadMF, WriteMF	MF 1 → Register 1 and 2
Integrated totals	**Register**	ReadCounter	Counter 1 → Register 1 and 2

Based on the above mapping table, we have to set **Object Point Numbers** in IEC 60870-5-104 as below:

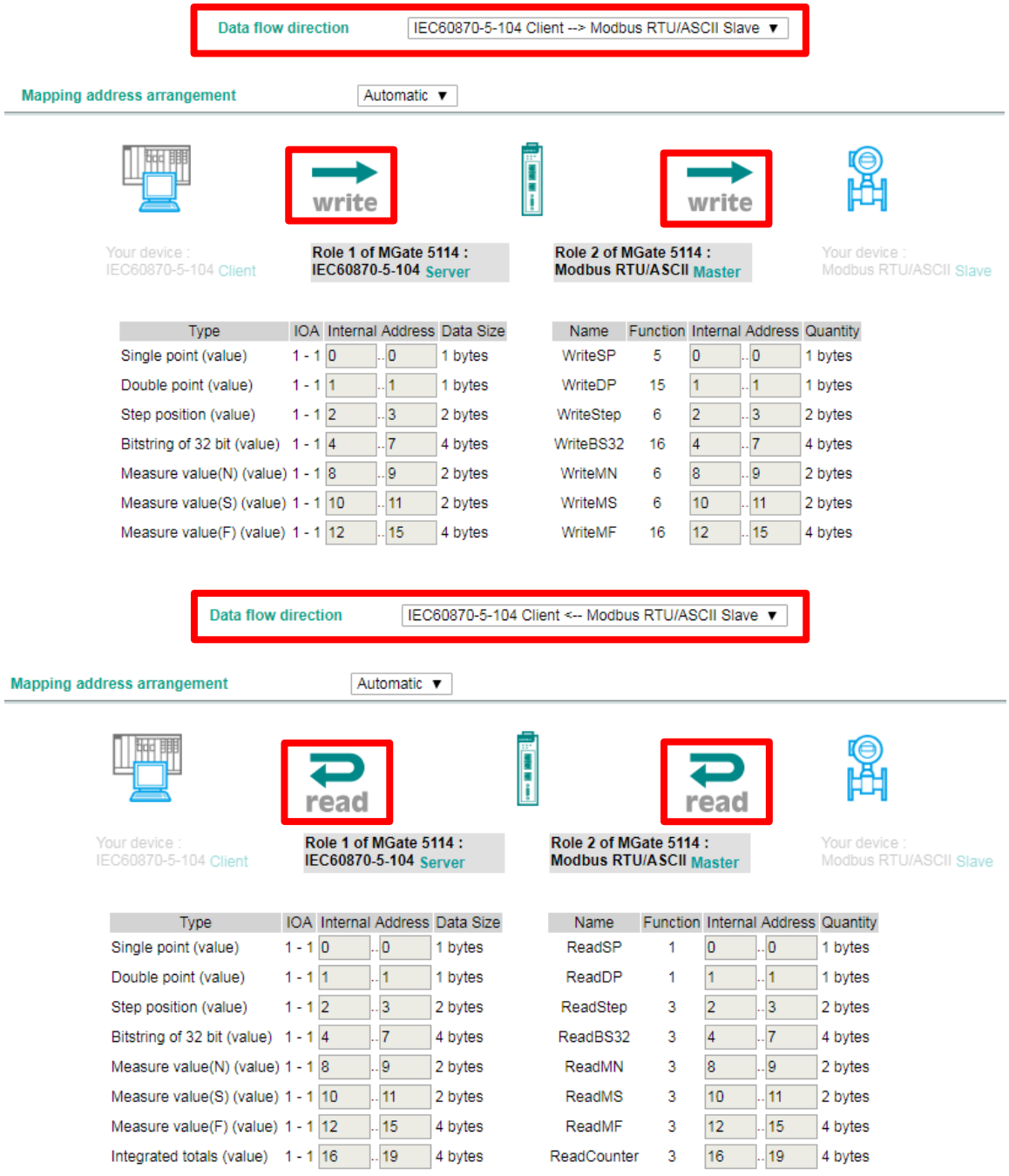
Point Settings

Add Edit Clone Delete Move

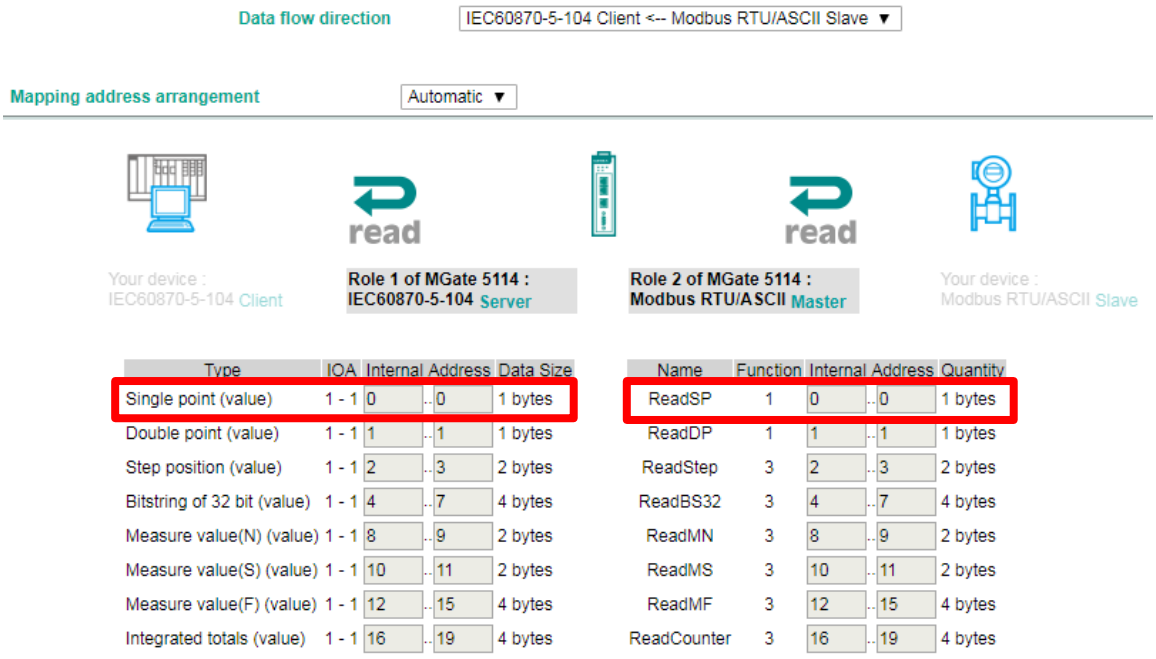
Index	Memory Access		Object Type	IOA
1	Read	Write	Single point	1 - 1
2	Read	Write	Double point	1 - 1
3	Read	Write	Step position	1 - 1
4	Read	Write	Bitstring of 32 bit	1 - 1
5	Read	Write	Measure value(N)	1 - 1
6	Read	Write	Measure value(S)	1 - 1
7	Read	Write	Measure value(F)	1 - 1
8	Read	Write	Integrated totals	1 - 1

Step 5. I/O Data Mapping

After protocol 1 and 2 settings, go to **I/O Data Mapping** to check whether the mapping table is correct. There are two dataflow directions; they are "Read" and "Write" respectively. In this table, make sure all of IEC 60870-5-104 object points are mapping to Modbus commands correctly.



For example, Modbus RTU Master sends a "ReadSP" to read the value from the Modbus slave device. If IEC 60870-5-104 Client wants to read the value through the "Single point IOA 1", **the settings of internal address should be the same**. If you want to make adjustments, please change the default arrangement "Automatic" to "Manual" first, then you can adjust the Internal Address.

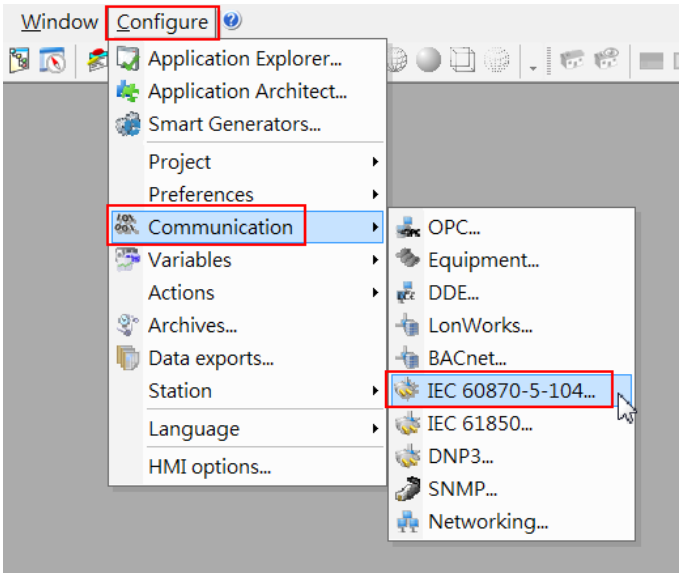


Type	IOA	Internal Address		Data Size
Single point (value)	1 - 1	0	0	1 bytes
Double point (value)	1 - 1	1	1	1 bytes
Step position (value)	1 - 1	2	3	2 bytes
Bitstring of 32 bit (value)	1 - 1	4	7	4 bytes
Measure value(N) (value)	1 - 1	8	9	2 bytes
Measure value(S) (value)	1 - 1	10	11	2 bytes
Measure value(F) (value)	1 - 1	12	15	4 bytes
Integrated totals (value)	1 - 1	16	19	4 bytes

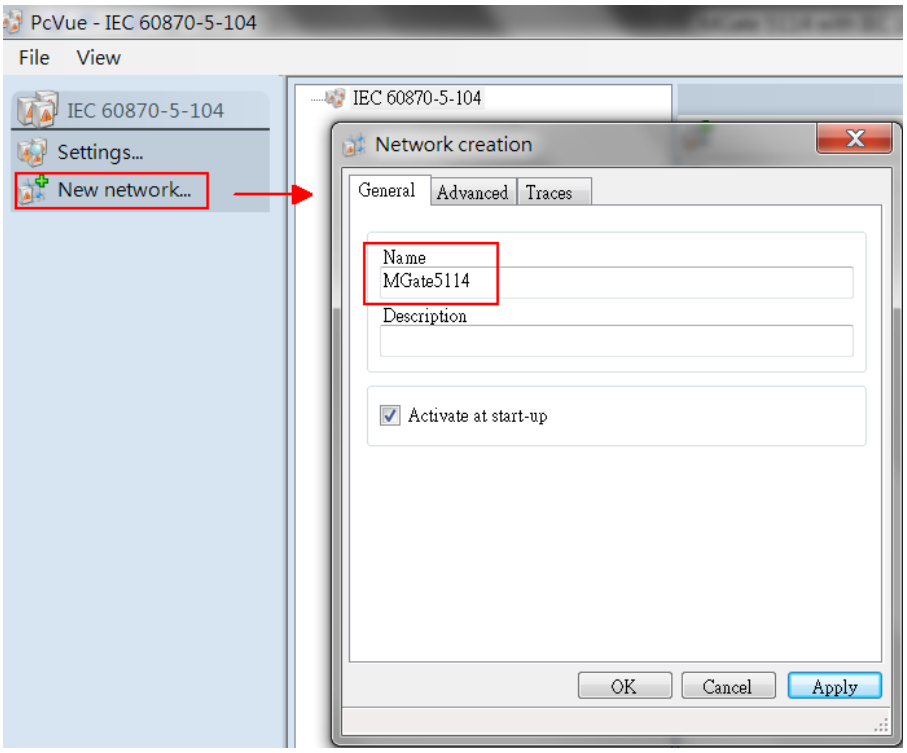
Name	Function	Internal Address		Quantity
ReadSP	1	0	0	1 bytes
ReadDP	1	1	1	1 bytes
ReadStep	3	2	3	2 bytes
ReadBS32	3	4	7	4 bytes
ReadMN	3	8	9	2 bytes
ReadMS	3	10	11	2 bytes
ReadMF	3	12	15	4 bytes
ReadCounter	3	16	19	4 bytes

5 Simulation of IEC 60870-5-104 Setting by PcVue

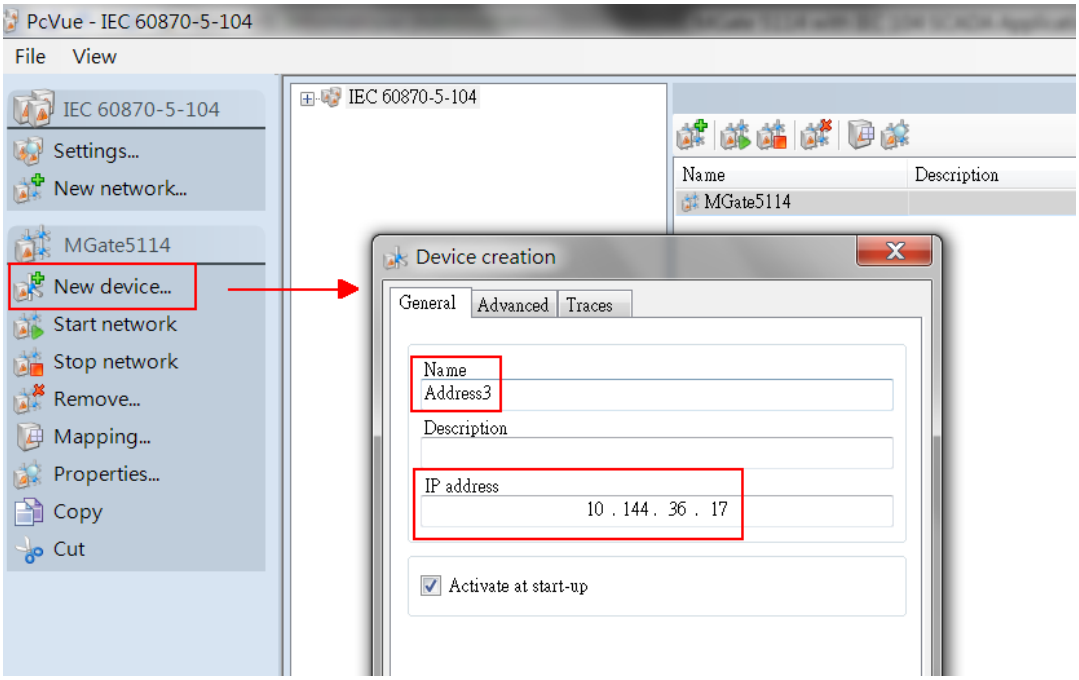
Here, PC1 runs PcVue as IEC 60870-5-104 Client, trying to connect the MGate 5114. The following shows how to configure IEC 60870-5-104 Client. For PcVue, click **Configure → Communication → IEC 60870-5-104** to establish a connection.



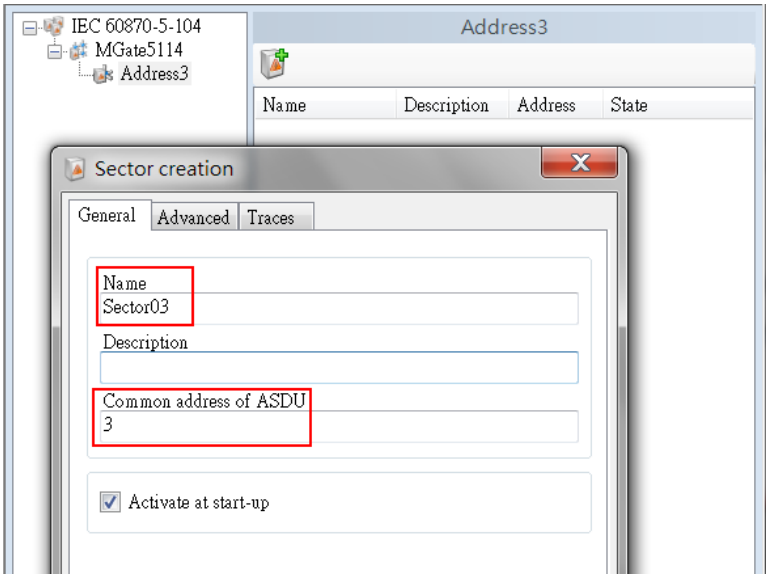
Click "**New network**" to add an IEC 60870-5-104 network.



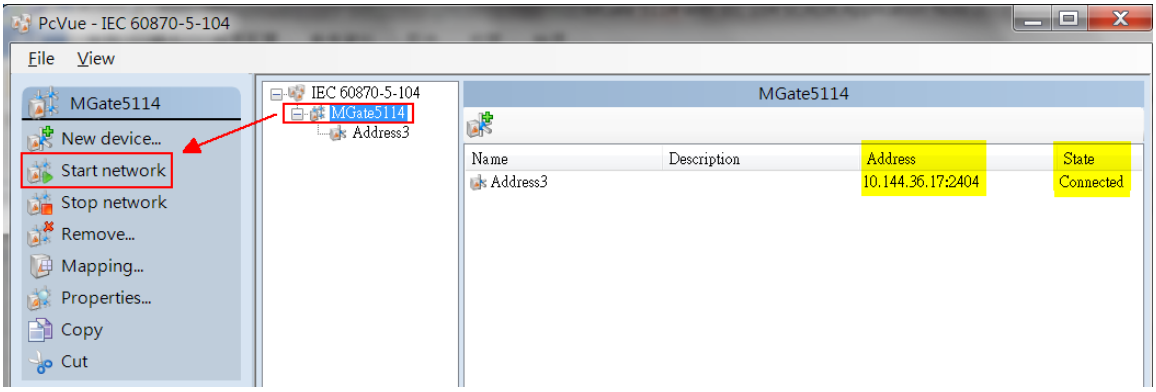
Click "**New device**" to create a device. Input name and input the MGate 5114's IP address.



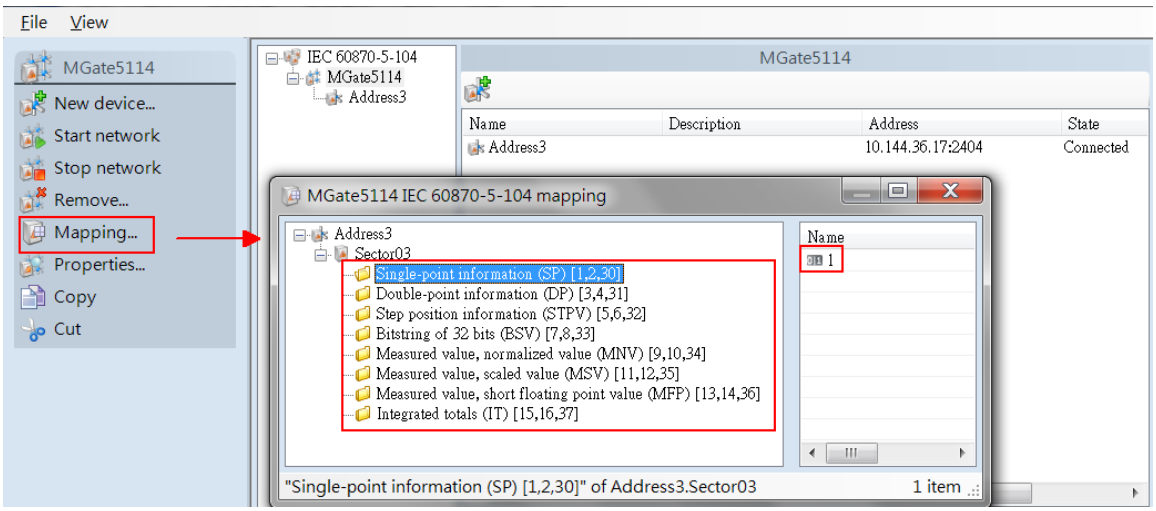
Click "**Add Sector**" to create a Sector. Input "Common address of ASDU" as 3, which is the same as that of the MGate 5114.



Select MGate5114 network, click "**Start network**" and SCADA will try to connect the MGate 5114. If the MGate 5114 is connected, the **State** would show "**Connected**".

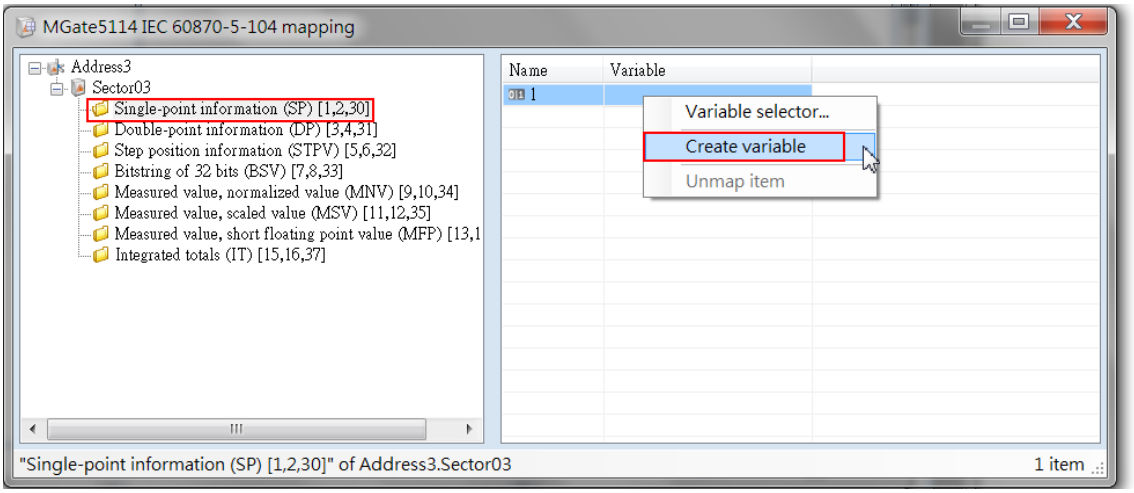


Click **Mapping** and an IEC 60870-5-104 object window will pop up. You can see several object points that are detected by the PcVue after making a connection according to the IEC 60870-5-104 communication characteristics. The objects include single-point information, double-point information, etc. They should be the same IEC 60870-5-104 server objects (MGate 5114).

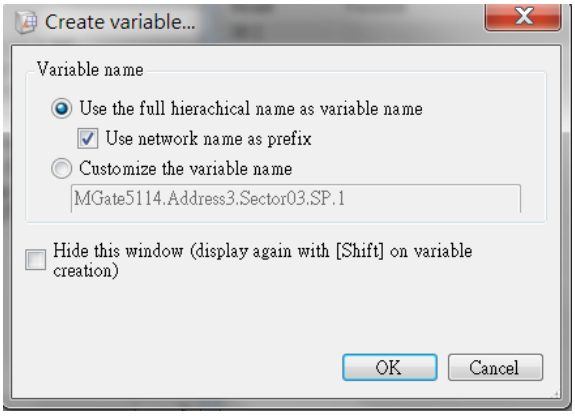


Create variables to show the values for these points with the following steps:

For example, choose Single Point IOA 1, right-click and select **"Create variable"**.

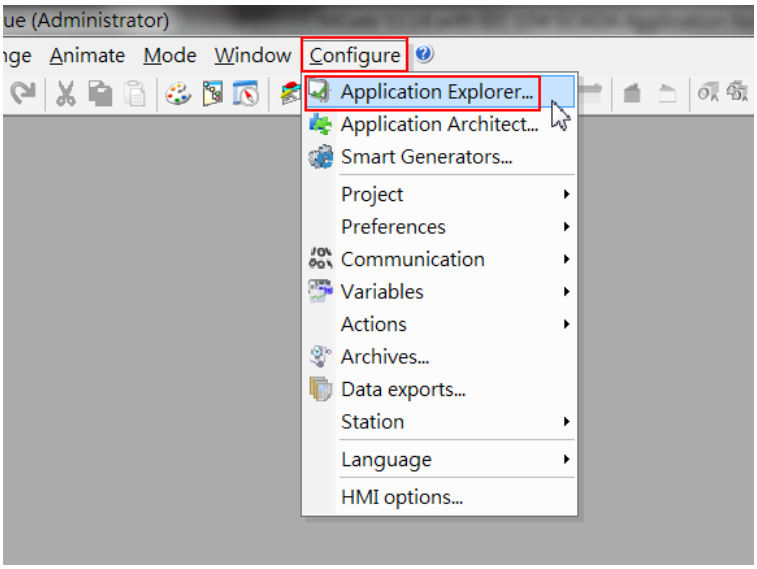


Choose **"Use the full hierarchical name"** and click **OK**.

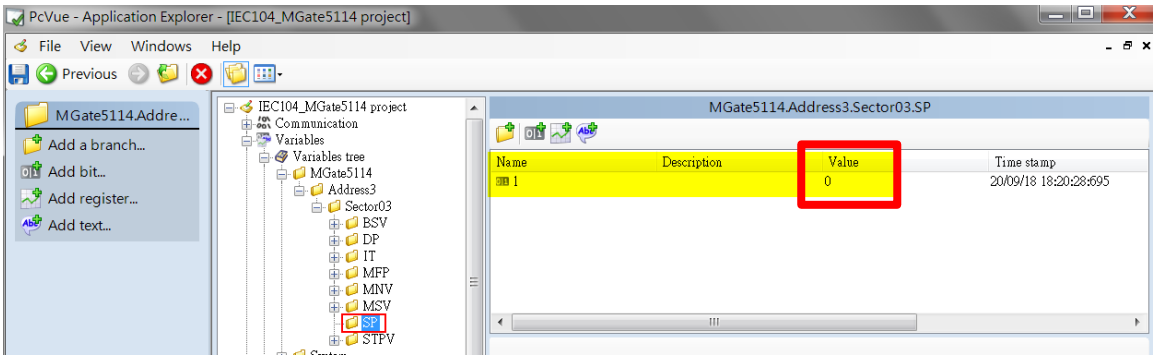


Use the same method to create variables for other object points.

Open Configure → Application Explorer Windows.



We can check each object's value as below:

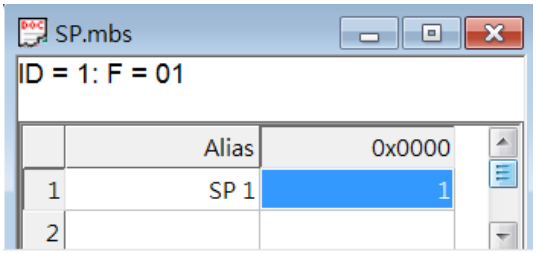


6 Communication Test

6.1 Read Single-Point Test

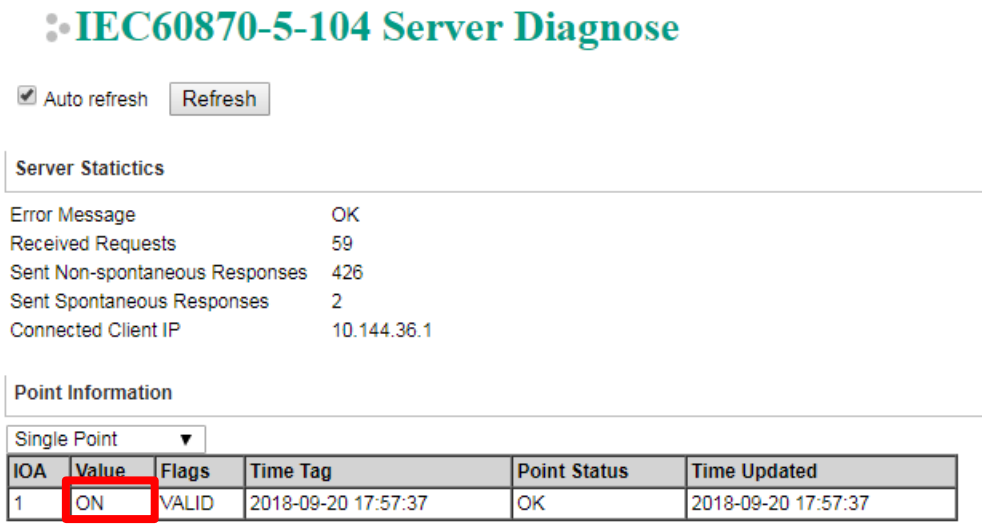
Modify Modbus Slave ID 1's Alias SP 1 status from 0(OFF) → 1(ON) as below:

< Modbus Slave-Single Point >



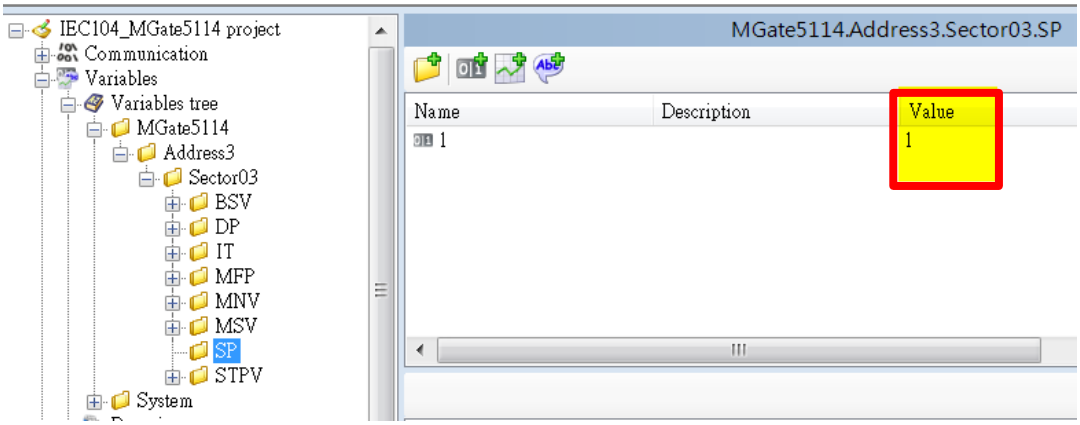
You can go to the Diagnose page to check whether the value has been updated in the MGate IEC 60870-5-104 server.

<MGate IEC 60870-5-104 Diagnose>



PcVue as IEC 60870-5-104 Client shows receiving the value "1(ON)" in the object.

< PcVue SCADA Single Point Status>



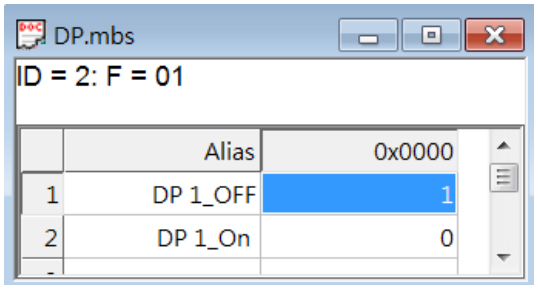
6.2 Read Double Point Test

Double point indicates 2-bit status; the status shows in the table below:

0 0	Indeterminate or intermediate state
1 0	Determined state **OFF (0)**
0 1	Determined state **ON (1)**
1 1	Indeterminate state

Modify Modbus Slave ID 2's Alias DP 1_Off status as "1" as below:

< Modbus Slave-Double Point >



Check the following status in the MGate's diagnose page

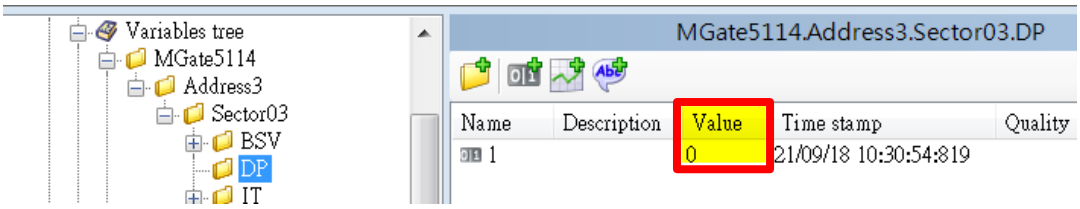
<MGate IEC 60870-5-104 Diagnose>

Point Information

Double Point

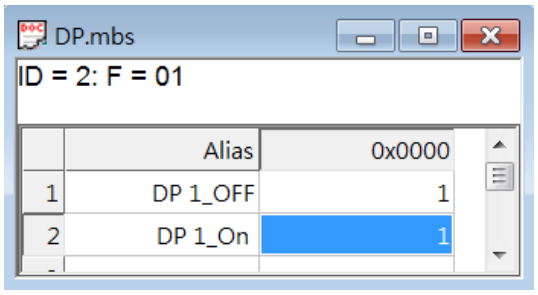
IOA	Value	Flags	Time Tag	Point Status	Time Updated
1	Off	VALID	2018-09-21 10:30:53	OK	2018-09-21 10:30:53

< PcVue SCADA Double Point Status >



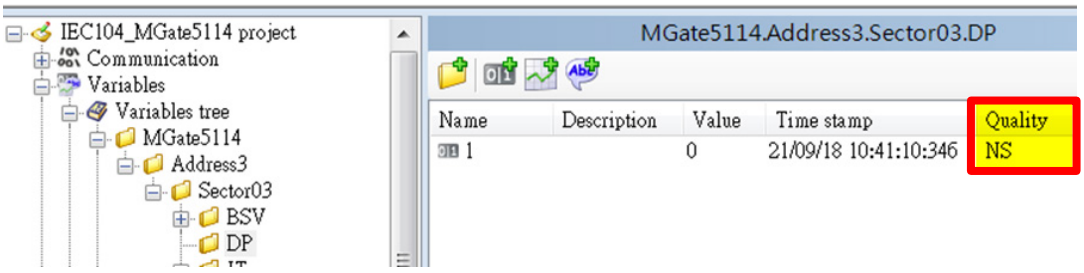
Modify Modbus Slave ID 2's Alias DP 1_On status as "1" as below:

< Modbus Slave-Double point >



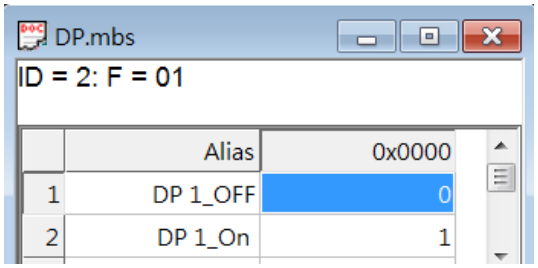
Check PcVue DP 1 status: its value is still 0, but Quality is "NS". It means this DP status is under "Indeterminate" State.

< PcVue SCADA Double Point Status >



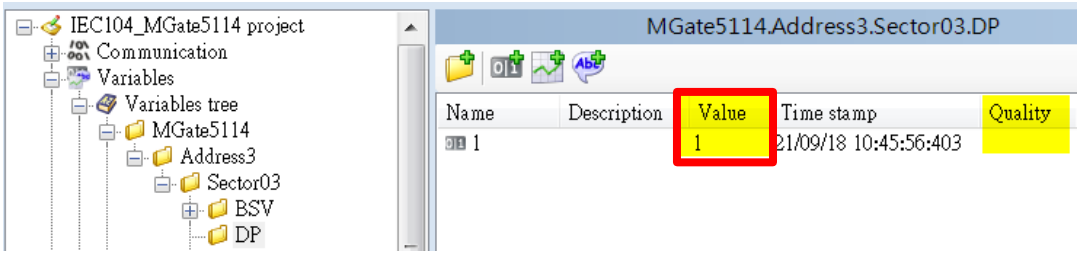
Modify Modbus Slave ID 2's Alias DP 1_OFF status as "0" as below:

< Modbus Slave-Double Point >



Check PcVue DP 1 status; its value is 1:

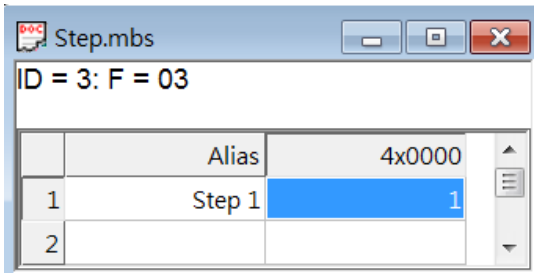
< PcVue SCADA Double Point Status >



6.3 Read Step Position Test

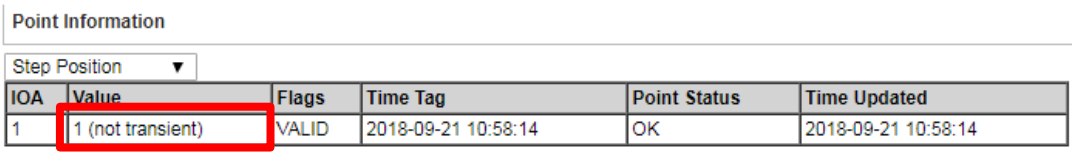
Modify Modbus Slave ID 3's Alias Step 1 status as "1" as below:

< Modbus Slave-Step Position Point>



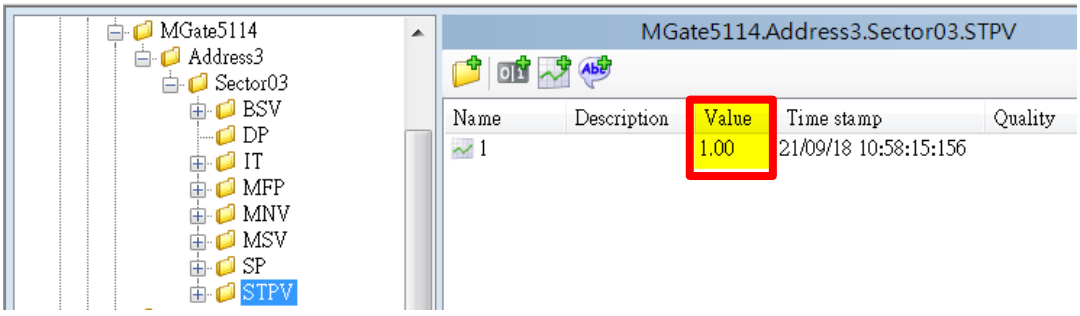
Check following status in the MGate's Diagnose page:

<MGate IEC 60870-5-104 Diagnose>



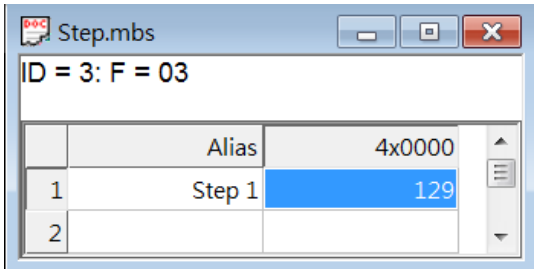
Check PcVue DP 1 status; its value is 1:

< PcVue SCADA Step Position Status >



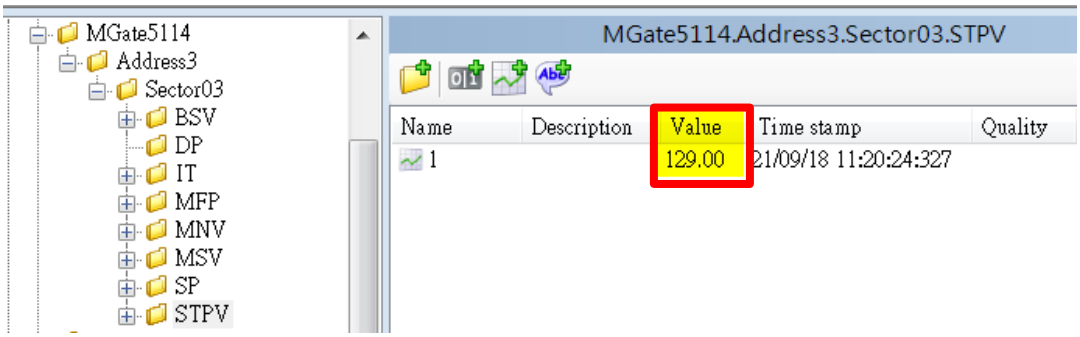
Modify Modbus Slave ID 3's Alias Step 1 status as "129" as below:

< Modbus Slave-Step Position Point >



PcVue shows this point's raw data as 129.

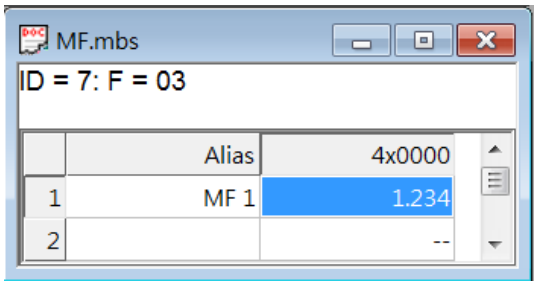
< PcVue SCADA Step Position Status >



6.4 Read MF Test

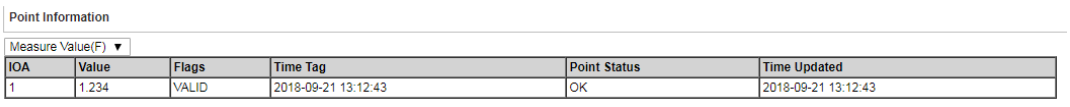
Modify Modbus Slave ID 7's Alias MF 1 status as "1.234" as below:

< Modbus Slave-MF Point >



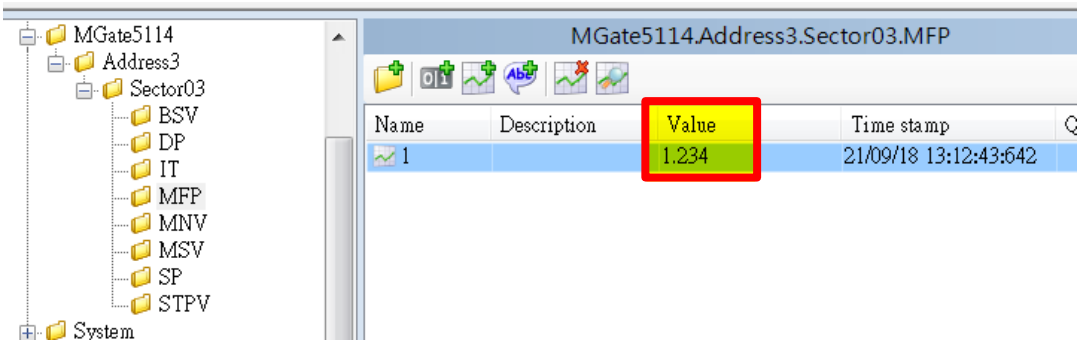
Check the following status in the MGate's diagnose page

<MGate IEC 60870-5-104 Diagnose>



The value has been changed to 1.234

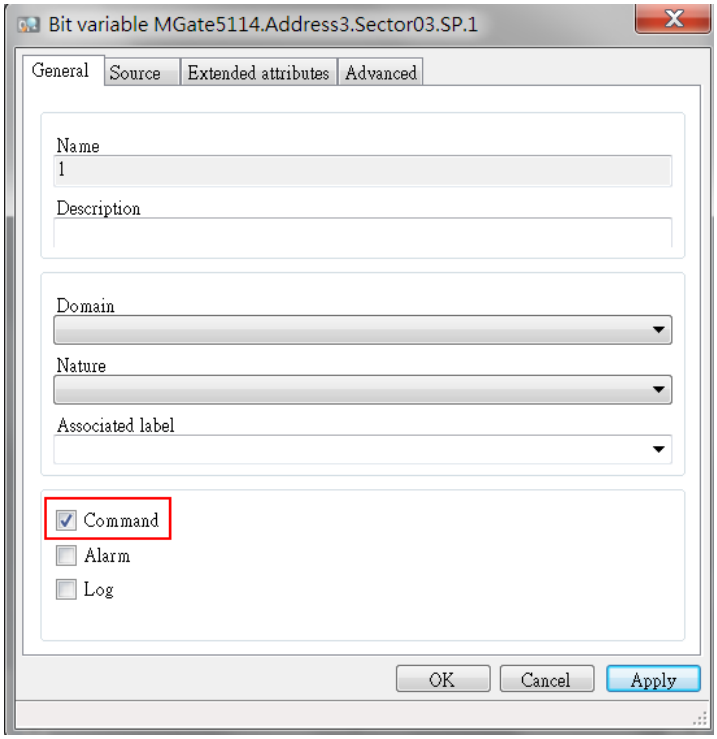
< PcVue SCADA Step Position Status >



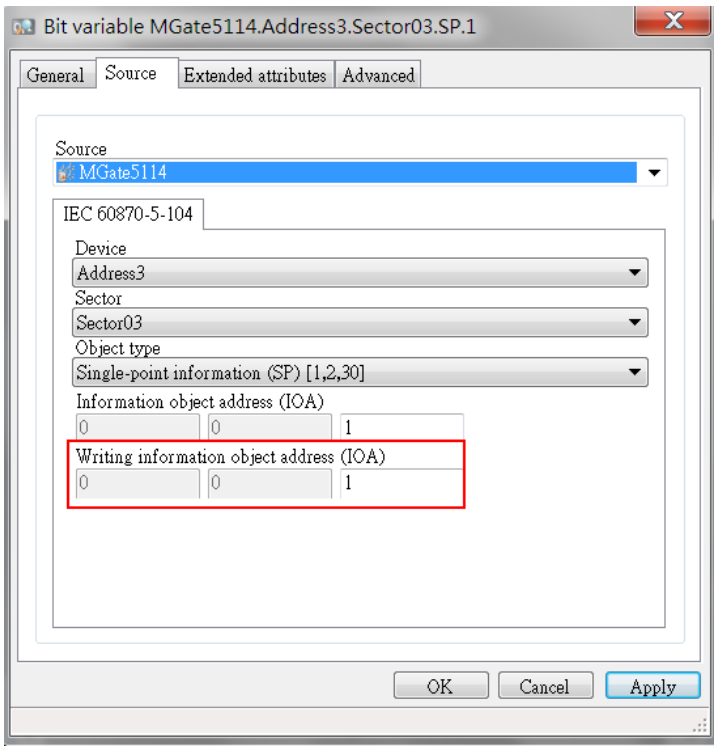
6.5 Write SP Test

In order for the variable to trigger a command, we should enable "Command" property.

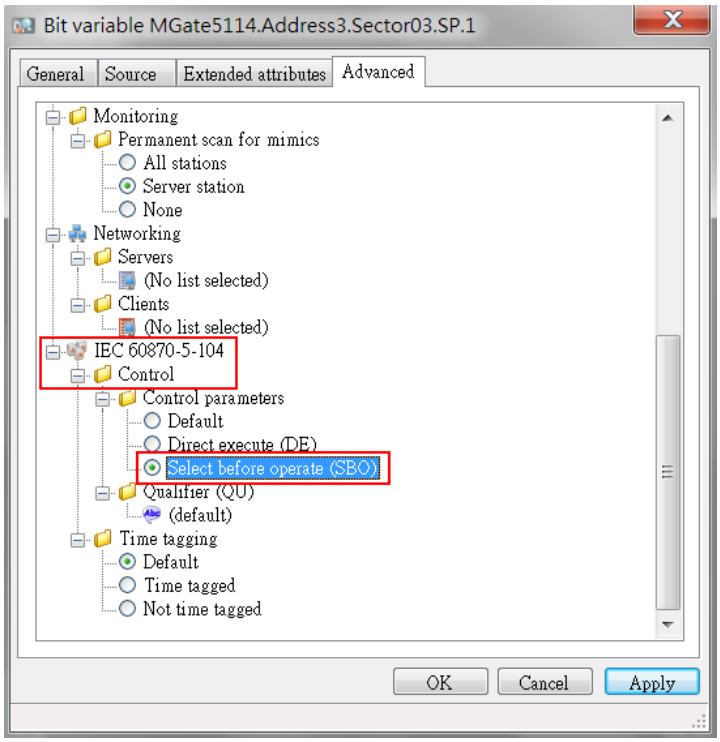
In the "General" tab, enable "Command".



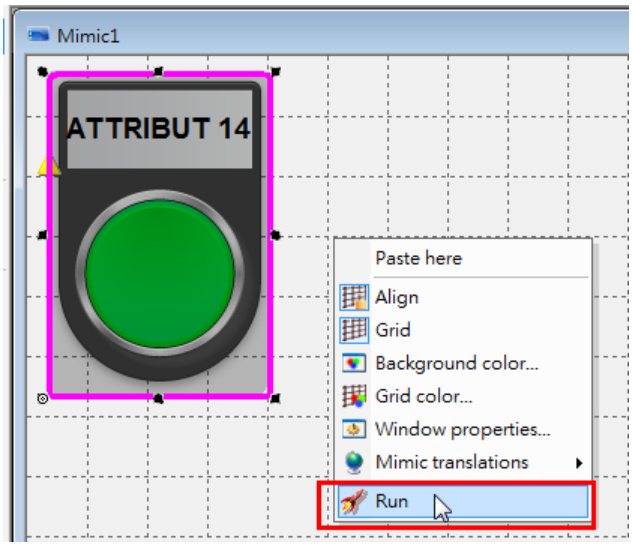
In the "Source" tab, modify "Write information object address (IOA)" as 1:



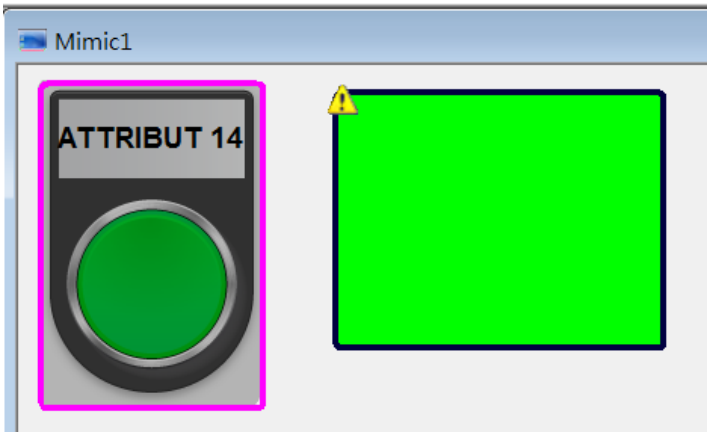
In the "Advanced" tab, choose "Select before operate (SBO)" under IEC 60870-5-104 → Control:



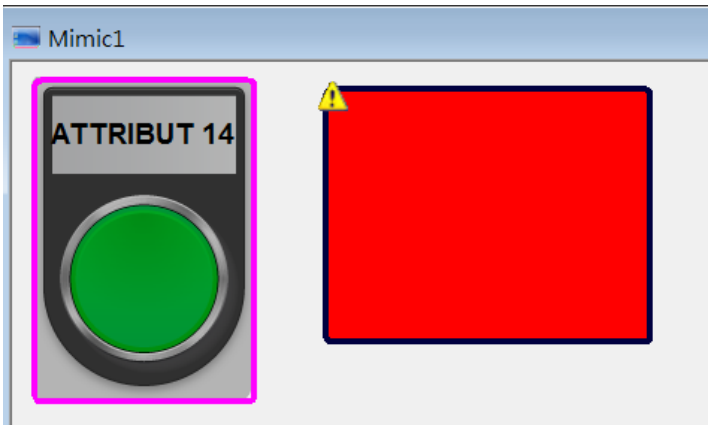
Right-click on Mimic to execute "**Run**" mode.



The rectangle will be Green, standing for SP 1 "1(On)".



Click the button, the rectangle will then be Red, standing for SP 1 "0(Off)".



We can then check the following status:

<MGate IEC 60870-5-104 Diagnose>

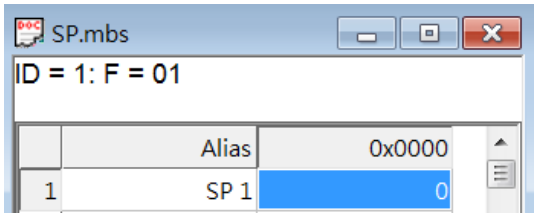
Point Information

Single Point

IOA	Value	Flags	Time Tag	Point Status	Time Updated
1	OFF	VALID	2018-09-21 16:23:00	OK	2018-09-21 16:23:01

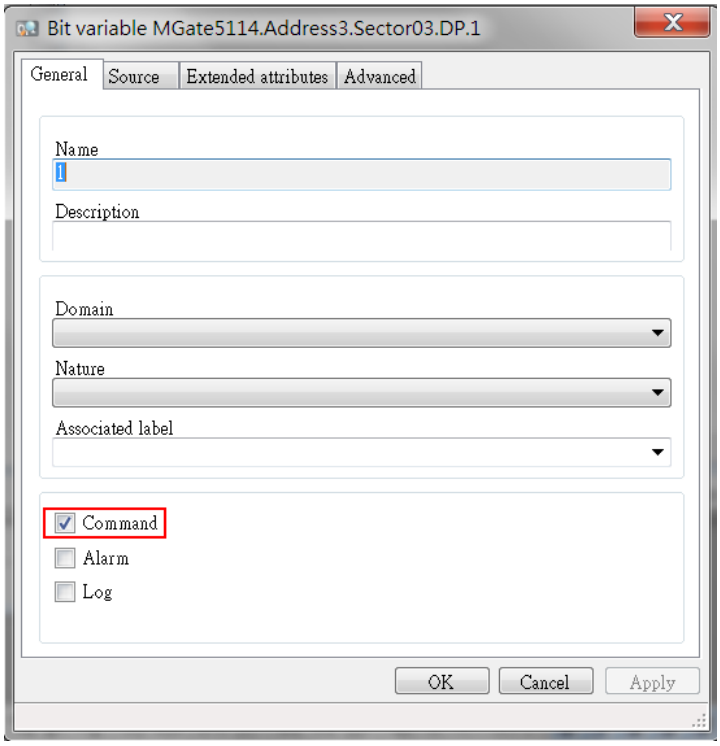
The value has been written to the Modbus Slave:

< Modbus Slave-Single Point >

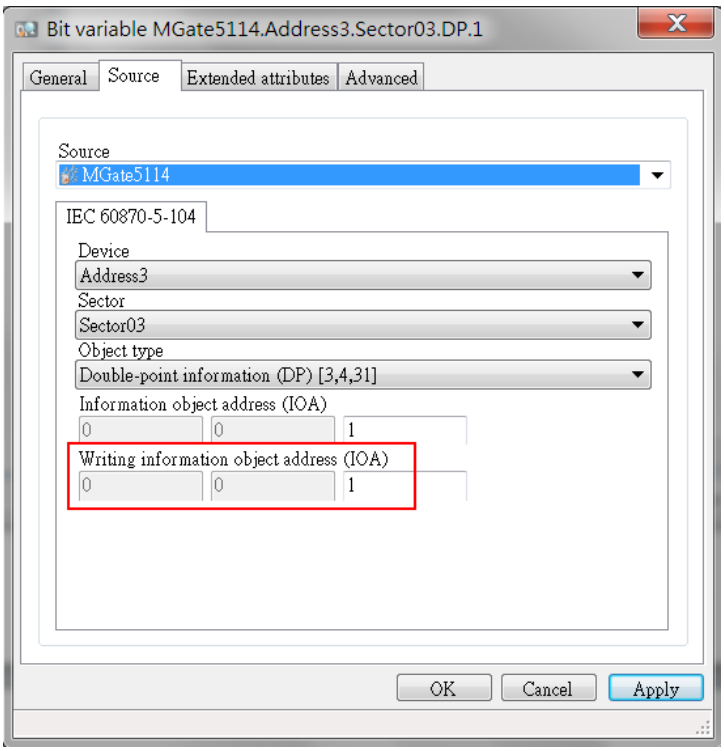


6.6 Write DP Test

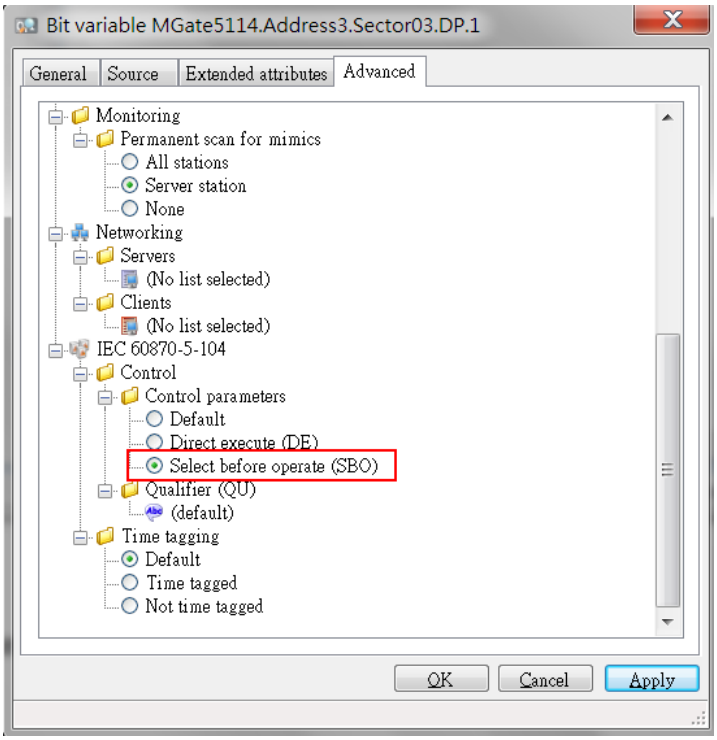
In DP 1's General tab, enable "Command".



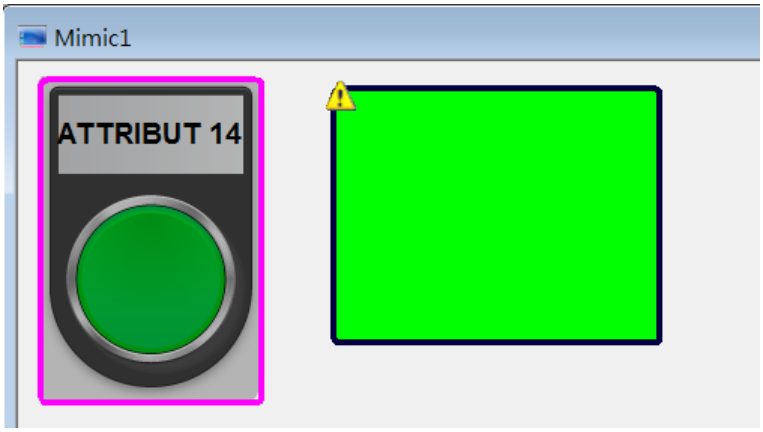
In the Source tab, modify "Write information object address (IOA)" as 1:



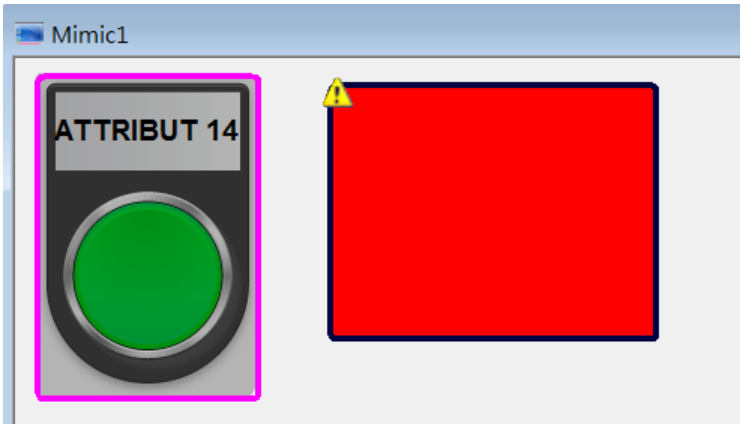
In the Advanced tab, choose "Select before operate (SBO)" under IEC 60870-5-104 → Control:



Right-click on Mimic to execute "**Run**" mode. The rectangle shows Green, standing for DP 1 "1(On)".



Click the button. The rectangle's turns Red, standing for DP 1 "0(Off)".



When Double Point shows "Off", we can check the following status:

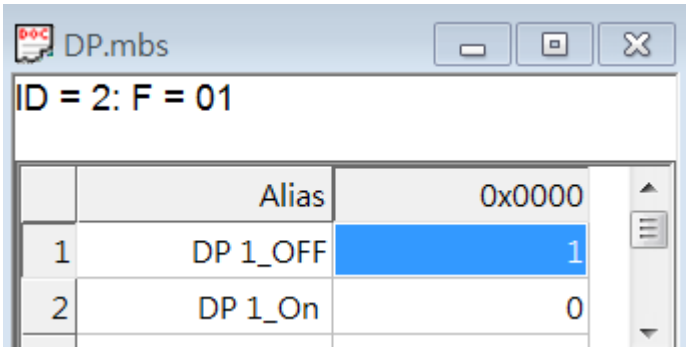
<MGate IEC 60870-5-104 Diagnose>

Point Information

Double Point ▼

IOA	Value	Flags	Time Tag	Point Status	Time Updated
1	Off	VALID	2018-09-21 17:03:06	OK	2018-09-21 17:03:07

< Modbus Slave-Double Point >

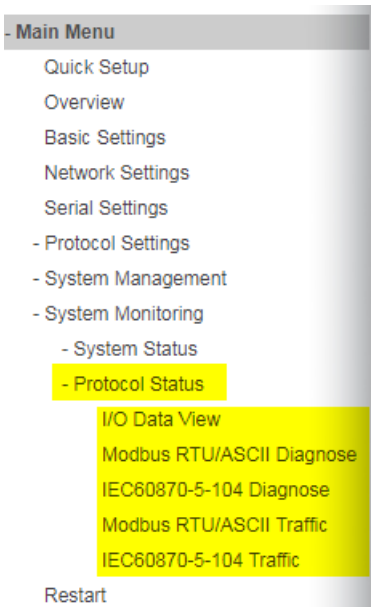


7 Troubleshooting Tool

7.1 MGate Protocol Diagnose Introduction

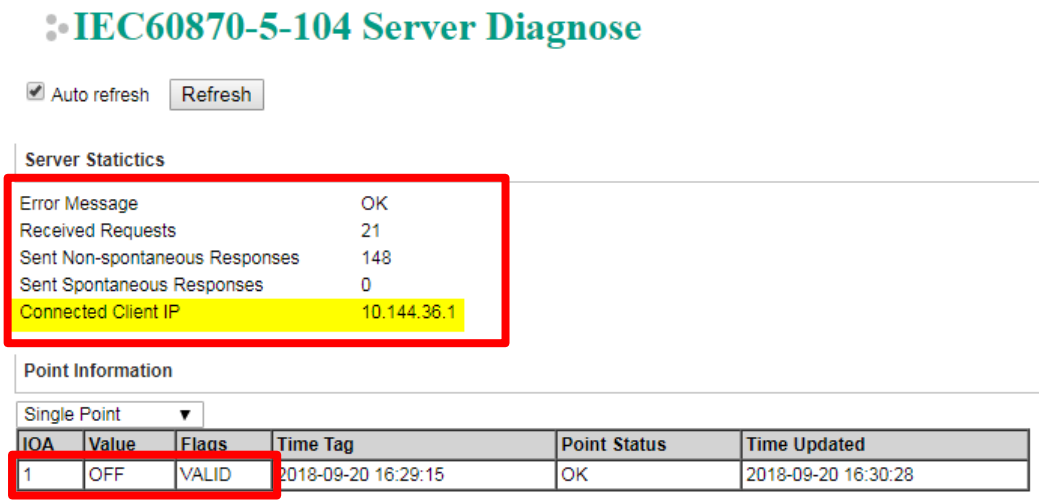
In the MGate 5114 web console, there is "**Protocol Status**" to diagnose Protocol Status, which include two powerful troubleshooting tools, "**Protocol Diagnose**" and "**Protocol Traffic**", as below:

< Protocol Status >



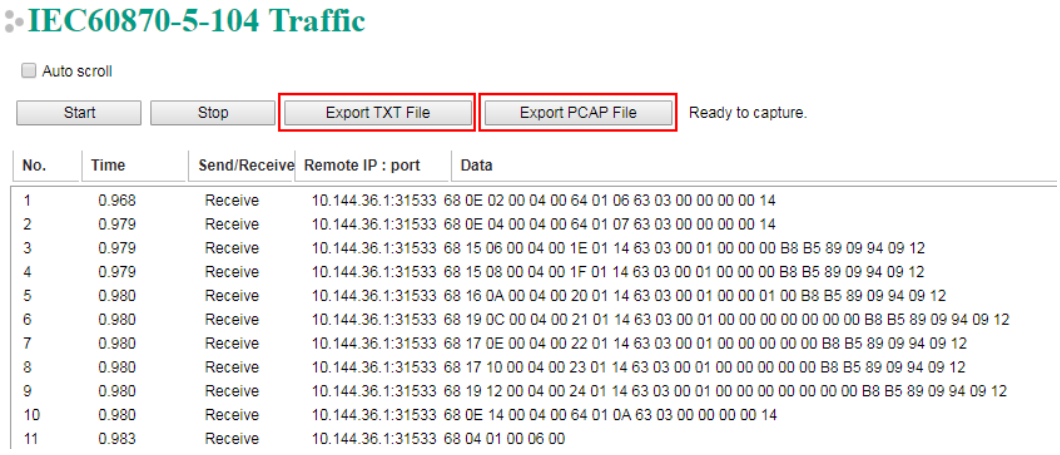
In the "**IEC 60870-5-104 Diagnose**" web page, we can monitor IEC 60870-5-104 Server connection status and the Object Points status.

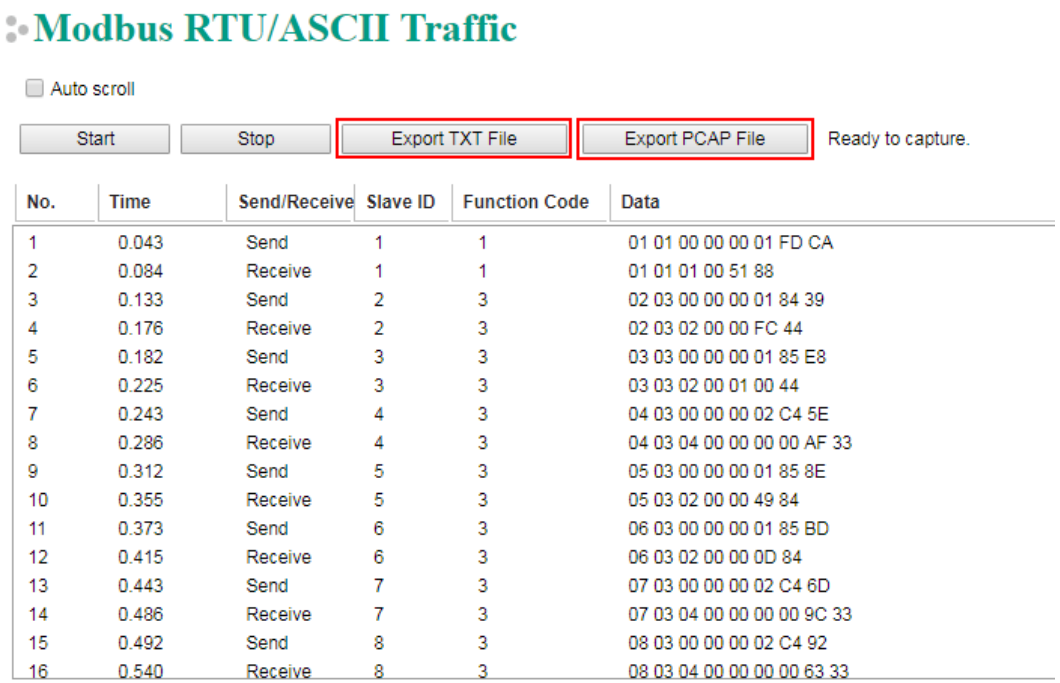
< IEC 60870-5-104 Server Diagnose >



7.2 MGate Traffic Monitor Introduction

In the "**IEC 60870-5-104 Traffic**" web page or "**Modbus RTU Traffic**" web page, these running communication traffics can be captured by clicking "Start". After clicking "Stop", we can export them in TXT file or PCAP file formats. the PCAP file can be executed by Wireshark tool, which helps to analyze the data easily.





Modbus RTU/ASCII Traffic

Auto scroll

Start | Stop | Export TXT File | Export PCAP File | Ready to capture.

No.	Time	Send/Receive	Slave ID	Function Code	Data
1	0.043	Send	1	1	01 01 00 00 00 01 FD CA
2	0.084	Receive	1	1	01 01 01 00 51 88
3	0.133	Send	2	3	02 03 00 00 00 01 84 39
4	0.176	Receive	2	3	02 03 02 00 00 FC 44
5	0.182	Send	3	3	03 03 00 00 00 01 85 E8
6	0.225	Receive	3	3	03 03 02 00 01 00 44
7	0.243	Send	4	3	04 03 00 00 00 02 C4 5E
8	0.286	Receive	4	3	04 03 04 00 00 00 00 AF 33
9	0.312	Send	5	3	05 03 00 00 00 01 85 8E
10	0.355	Receive	5	3	05 03 02 00 00 49 84
11	0.373	Send	6	3	06 03 00 00 00 01 85 BD
12	0.415	Receive	6	3	06 03 02 00 00 0D 84
13	0.443	Send	7	3	07 03 00 00 00 02 C4 6D
14	0.486	Receive	7	3	07 03 04 00 00 00 00 9C 33
15	0.492	Send	8	3	08 03 00 00 00 02 C4 92
16	0.540	Receive	8	3	08 03 04 00 00 00 00 63 33