

Chapter 15 Modbus RTU

15.1 Modbus Protocol Outline

MODBUS protocol that is the specified open protocol used for server-client is operated by data reading/writing based on function code. The communication that adopts MODBUS protocol applies server-client function dealt with only one client.

Characteristics		RTU Mode
Signal system		8 bit binary code
The number of data per 1 character	Starting bit	1
	Data bit	8
	Parity bit	Even, Odd, None
	Stop bit	1 or 2
Error check		CRC (Cyclical Redundancy Check)
Start of frame		3.5 Characters no response time

15.1.1 Frame Structure

The frame structure of MODBUS RTU mode is as below.

Classification	Start	Station No.	Function code	Data	Error check	End
Size(byte)	Idle time	1	1	N	2	Idle time

- (1) Characteristics of RTU mode
 - It adopts hexadecimal number for communication.
 - Starting character indicates unit No. and the end of frame indicates CRC error check for identifying the frame.
 - It identifies start and end of the frame by adding idle time of 1 bit.
 - It has at least 3.5 character time of interval between frames and when passing 1.5 character times, it is regarded as independent frame.
- (2) Address Area
 - It is composed of 1 byte.
 - When using XGT Cnet I/F module, 0~31 can be applied for the unit No.
 - 0 is used for client local number.
 - Server includes its address to the response frame to show a client's response.
- (3) Data Area
 - It transmits data through hexadecimal number(Hex.) and data structure changes depending on each function code.
 - It replies with response data when receiving normal frame.

- It replies with error code when receiving abnormal frame.

(4) Error Check Area

- Through CRC checking method of 2 byte, it judges whether the frame is normal or not

(5) MODBUS Address Regulations

- The address of data starts from 0 and it is equal to the value obtained by subtracting 1 from MODBUS memory. Namely, MODBUS address 2 is the same as address 1 of data.

15.1.2 Displaying Data and Address

In terms of displaying data and address of MODBUS protocol, the main characteristics are as below.

- It basically adopts hexadecimal number(Hex.).
- The meaning of each function code is as below.

Code(Hex)	Used for	Using area	Address	Max. Response data
01	Reading individual /continuous bit	Bit output	0XXXX	2000Bit
02	Reading individual /continuous bit	Bit input	1XXXX	2000 Bit
03	Reading individual /continuous word	Word output	4XXXX	125 Word
04	Reading individual /continuous word	Word input	3XXXX	125 Word
05	Writing individual bit	Bit output	0XXXX	1 Bit
06	Writing individual word	Word output	4XXXX	1 Word
0F	Writing continuous bit	Bit output	0XXXX	1968 Bit
10	Writing continuous word	Word output	4XXXX	120 Word

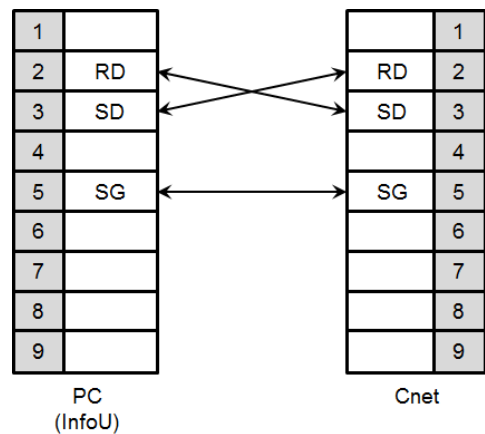
15.2 Wiring Diagram

The wiring method of InfoU and PLC connected through MODBUS communication may be different depending on the manufacturer. For proper wiring, refer to each PLC's manual.

The description on wiring of LS Industrial Systems' XGT PLC will be provided hereupon.

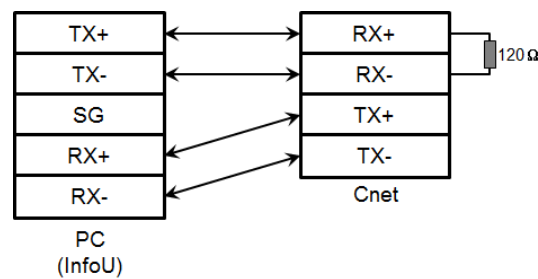
15.2.1 RS-232C

When connecting MODBUS communication through RS-232C mode, the wiring method is the same as general wiring method for RS-232C.



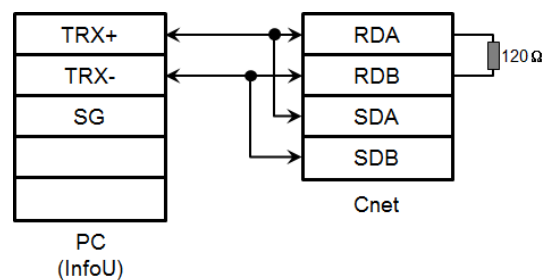
15.2.2 RS-422

When connecting MODBUS communication through RS-422 mode, the wiring method is the same as general wiring method for RS-422.



15.2.3 RS-485

When connecting MODBUS communication through RS-485 mode, the wiring method is the same as general wiring method for RS-485.

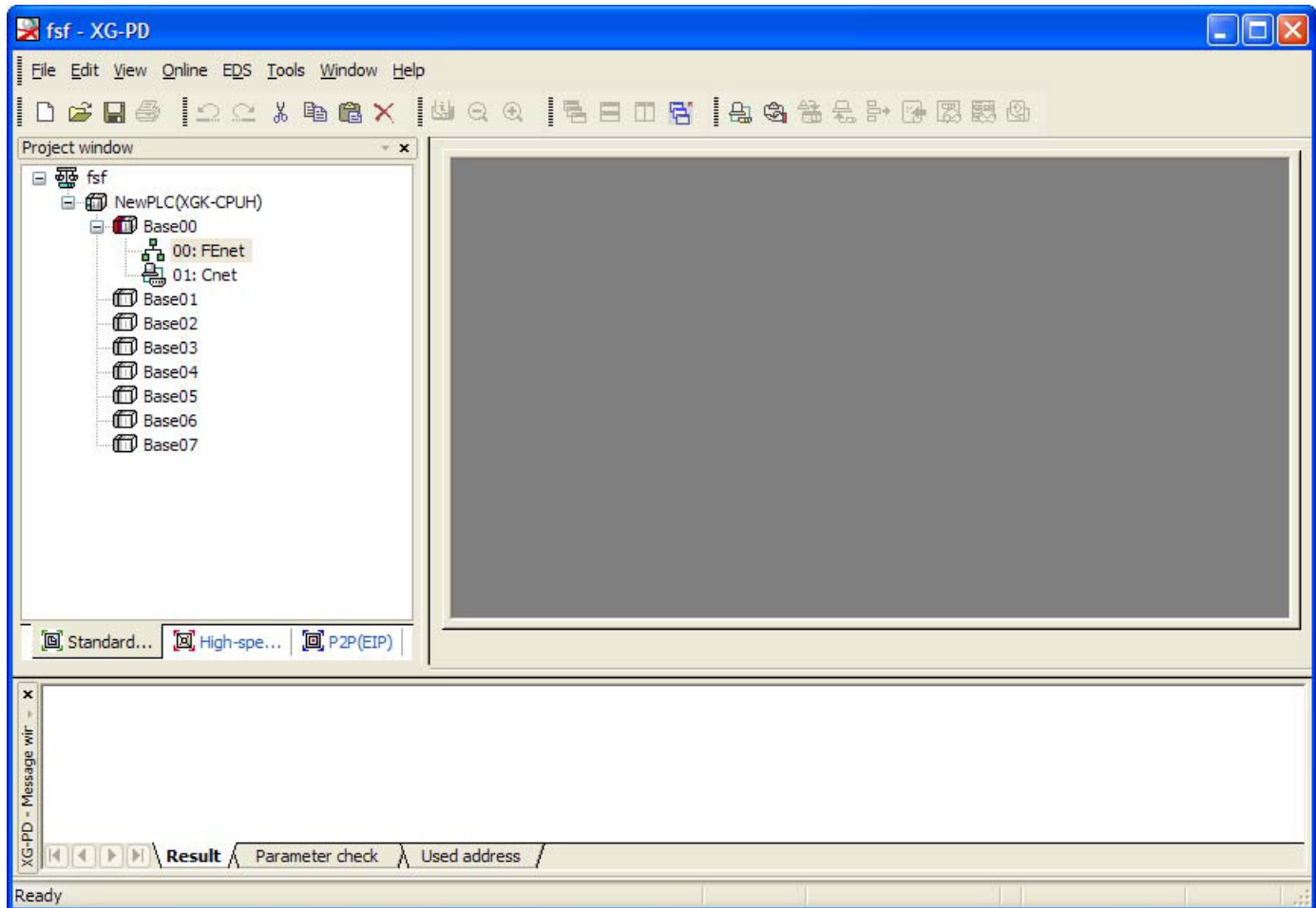


15.3 I/O Driver Setting

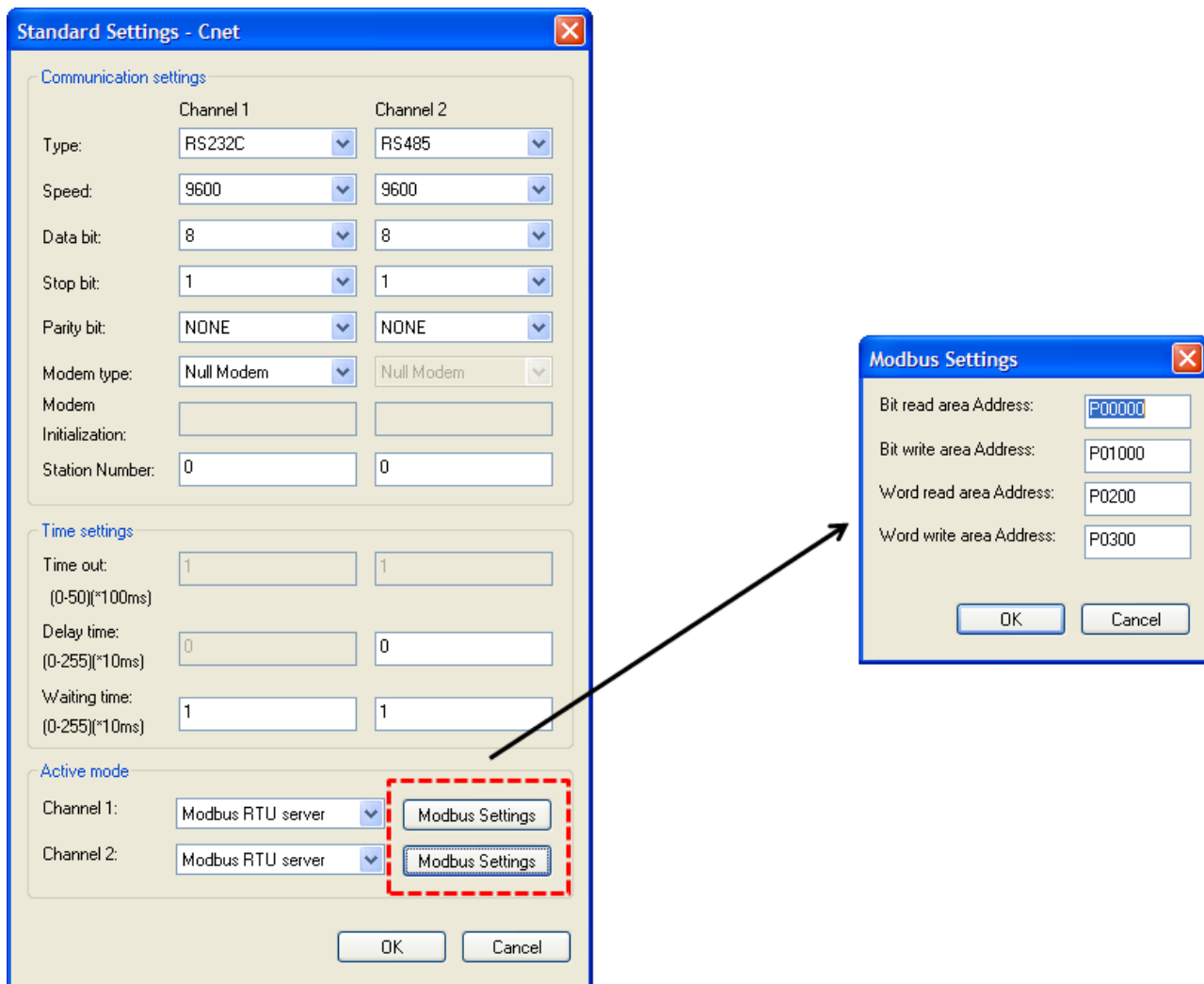
InfoU can be connected through various kinds of devices that adopt MODBUS(RTU) communication with RS-232C, RS-422/485 mode. Setting methods are different depending on the manufacturer so for more details, refer to each device manual. For example, description on XGK PLC will be provided hereupon.

15.3.1 PLC Setting

The communication for PLC(XGK) is set at XG-PD.



- (1) Connection Setting
 - Select [Online] → [Connection Setting].
 - After setting connection options for user environment, click Connection.
- (2) Reading I/O Data
 - Select [Online] → [Reading I/O Data] to interpret the information of module embedded in the current base.



(3) Basic setting

- Double-click the related Cnet I/F module to execute basic setting screen and establish communication mode, communication speed, modem type, data bit, stop bit, unit No. of connection setting menu.

(4) Operation mode

- Select RTU server for operation mode.
- If you select MODBUS RTU server for operation mode, executing MODBUS is active.

(5) Setting MODBUS

- Starting address of bit reading area : Indicates the starting address of bit reading area with 5 digits. The former 4 digits indicate word value and the remaining 1 digit means bit value.

Ex.) In the case of M00000 : The 0th bit of 0th word of M device is set as starting address of bit reading area.

- Starting address of bit writing area : Indicates the starting address of bit writing area with 5 digits. The former 4 digits indicate word value and the remaining 1 digit means bit value.

In the case of M00100: The 0th bit of 10th word of M device area is set as starting address of bit reading area.

- Starting address of word reading area: Indicates the starting address of word reading area with 4 digits.
Ex.) In the case of M00200: The 200th word of M device area is set as starting address of word reading area.
- Starting address of word writing area: Indicates the starting address of word writing area with 4 digits.
Ex.) In the case of M00300: The 300th word of M device area is set as starting address of word writing area.

(6) Writing Parameter

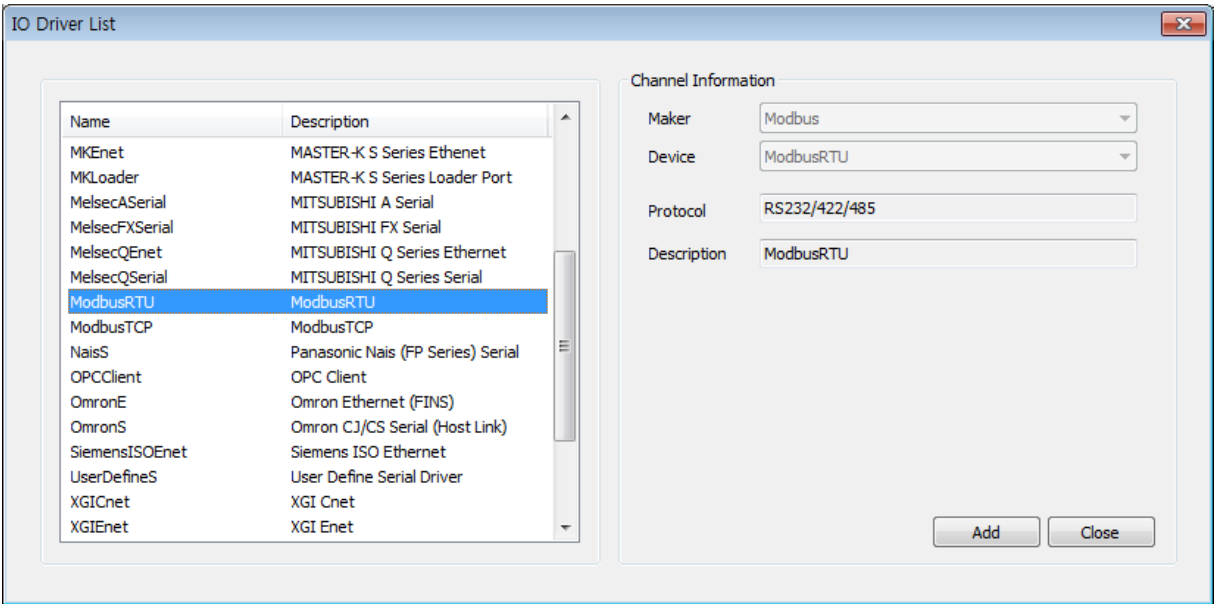
- Click [Online] → [Writing parameter].
- After clicking the module whose basic setting is completed at basic setting, click OK button.
- After clicking OK button, complete Parameter Writing and reset the module individually.

(7) Checking operation

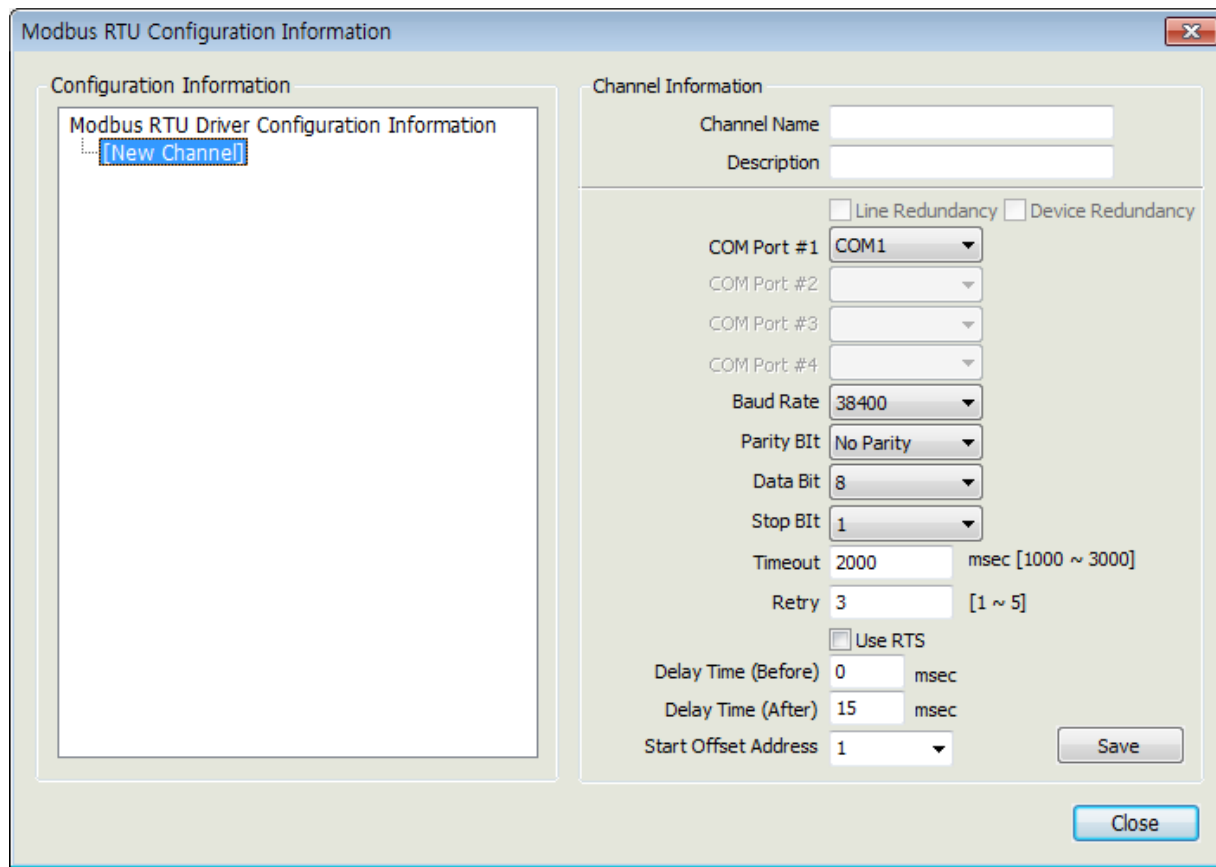
- Click [Online] → [System Diagnosis].
- After clicking the related module, press the right mouse button for frame monitoring and status by services to check whether communication is normal or not.

15.3.2 InfoU Setting: ModbusRTU

(1) Add Channel



Select “ModbusRTU” from the I/O driver list and press “Add”.



The dialog box is titled "Modbus RTU Configuration Information". It is divided into two main sections: "Configuration Information" on the left and "Channel Information" on the right.

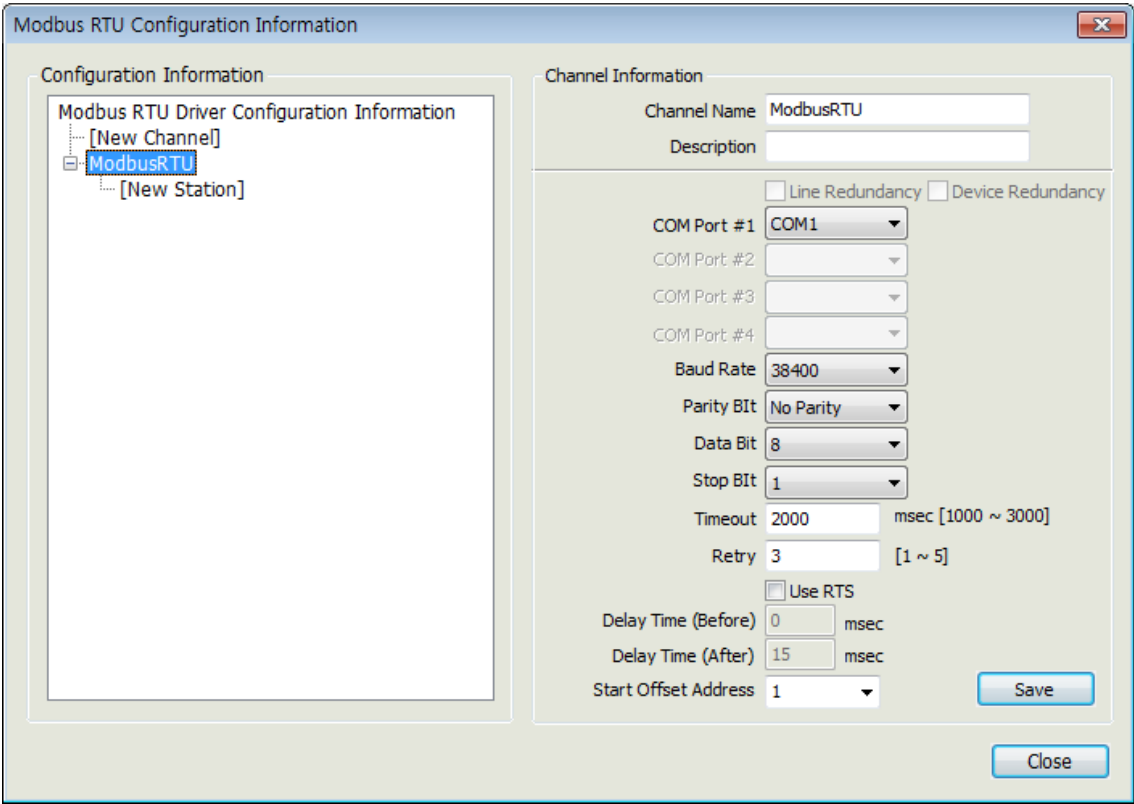
Configuration Information: This section contains a tree view labeled "Modbus RTU Driver Configuration Information". A button labeled "[New Channel]" is visible at the top of the tree.

Channel Information: This section contains various input fields and checkboxes for configuring a channel.

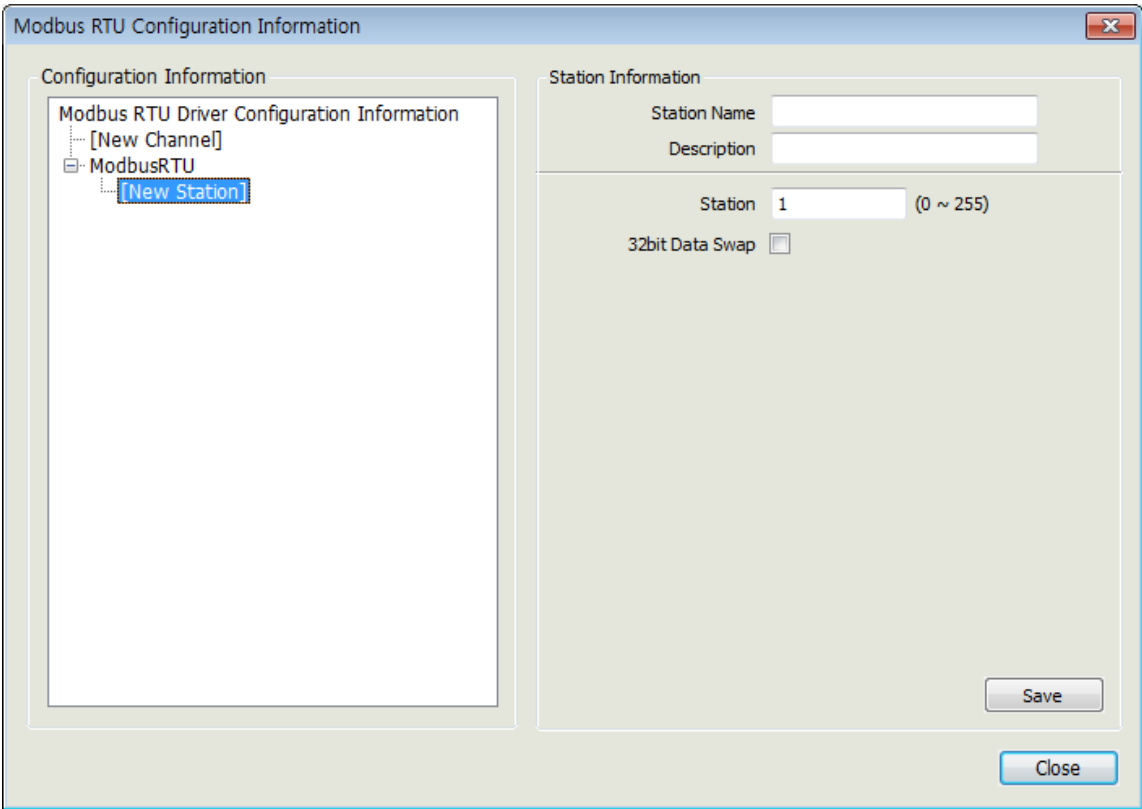
- Channel Name:** A text input field.
- Description:** A text input field.
- Line Redundancy:** A checkbox.
- Device Redundancy:** A checkbox.
- COM Port #1:** A dropdown menu currently showing "COM1".
- COM Port #2:** A dropdown menu.
- COM Port #3:** A dropdown menu.
- COM Port #4:** A dropdown menu.
- Baud Rate:** A dropdown menu currently showing "38400".
- Parity Bit:** A dropdown menu currently showing "No Parity".
- Data Bit:** A dropdown menu currently showing "8".
- Stop Bit:** A dropdown menu currently showing "1".
- Timeout:** A text input field showing "2000" with the unit "msec" and a range "[1000 ~ 3000]".
- Retry:** A text input field showing "3" with a range "[1 ~ 5]".
- Use RTS:** A checkbox.
- Delay Time (Before):** A text input field showing "0" with the unit "msec".
- Delay Time (After):** A text input field showing "15" with the unit "msec".
- Start Offset Address:** A dropdown menu currently showing "1".

At the bottom right of the "Channel Information" section are two buttons: "Save" and "Close".

- Channel Name: Input a channel name.
- Description: Input some information on the channel.
- COM Port #1: Select a communication port.
- Baud Rate: Select a communication speed.
- Parity Bit: Select a parity bit.
- Data Bit: Select a data bit.
- Stop Bit: Select a stop bit.
- Time Out : It refers to a certain time period during which any response to the request for data is not made and after passing such a time period, the system will declare timeout to move on to the next process. The time period to be set will be a base to judge communication errors.
- Retry: Set up the number of times to retry when communication fails.
- Use RTS: Check ☒ in the box only when using Channel 485 and 422.
- Delay Time (Before): Information used only in Channel 485 and 422. The delay time right before requesting Data to PLC.
- Delay Time (After): Information used only in Channel 485 and 422. The delay time right after requesting Data to PLC
- Start Offset Address: Select either 0 or 1. It sets up whether to start from either 0 or 1.
- Save: If 'Save' button is pressed, Channel information will be saved and the saved information will add to the left "Configuration Information" tree.

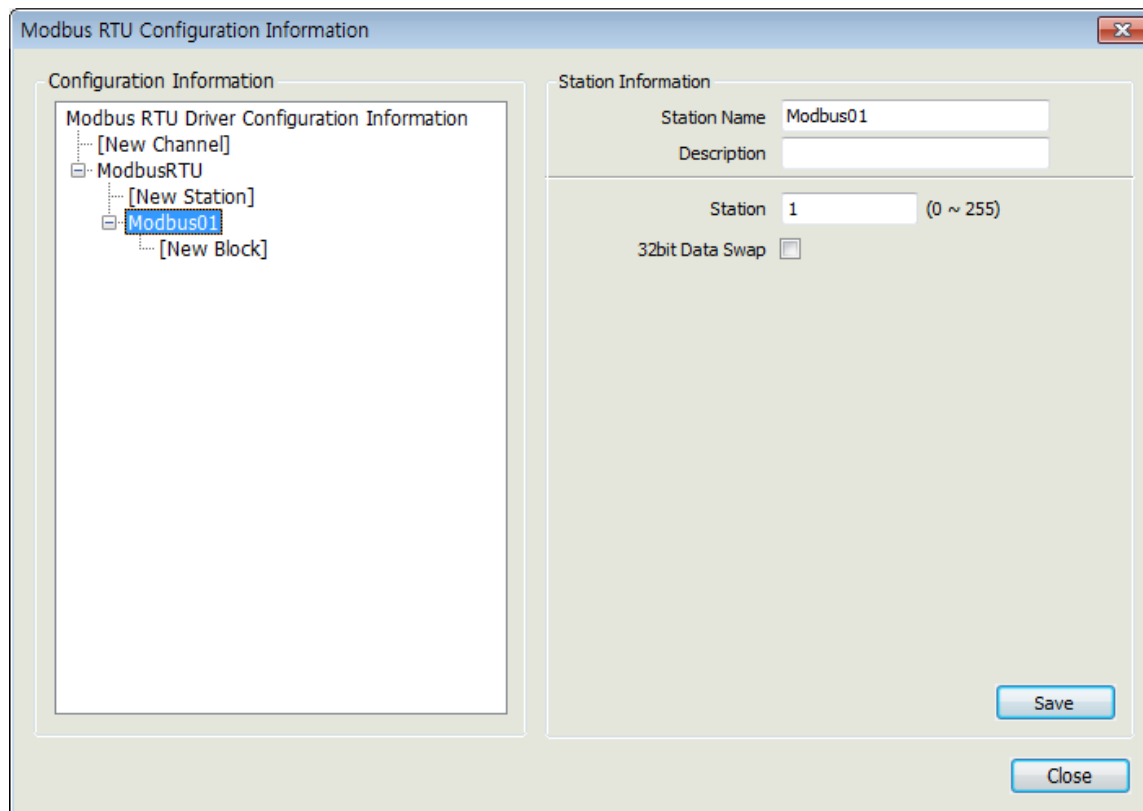


(2) Add Station

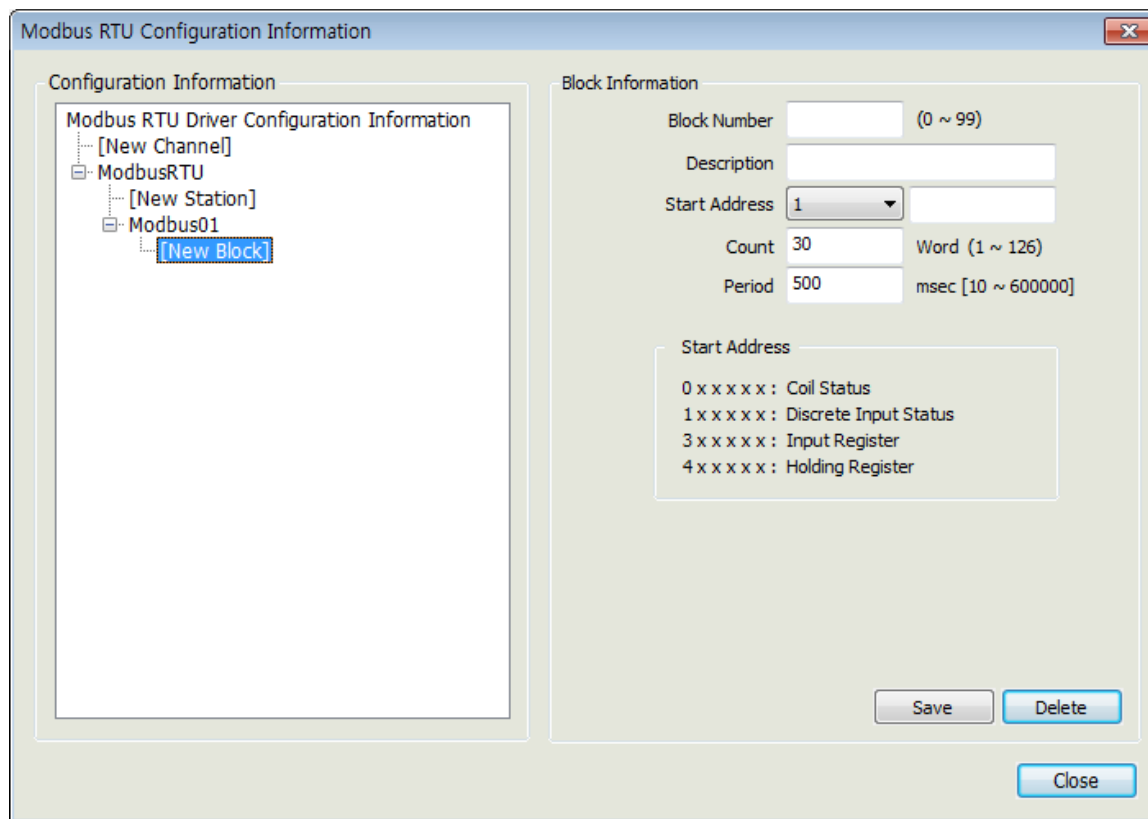


- Select [New Station] from “Configuration Information” tree.

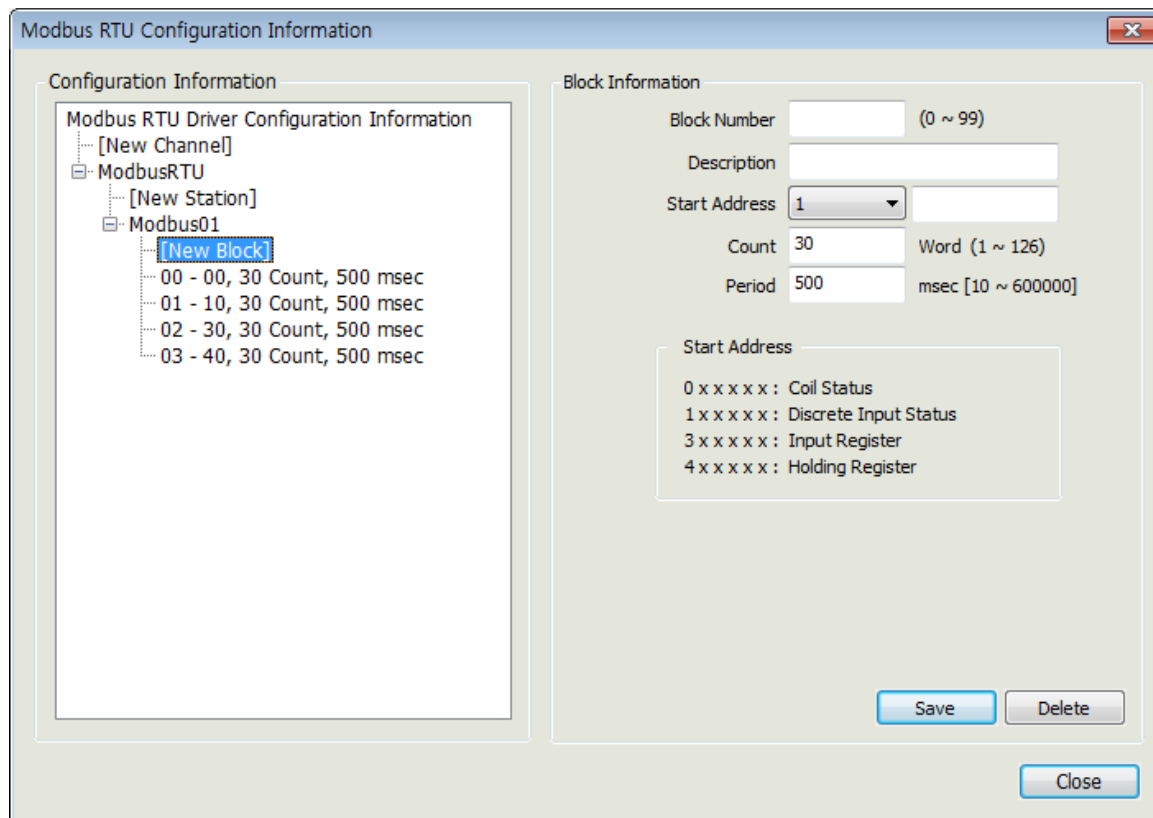
- Station Name: Input a station name.
- Description: Input some information on the station.
- Station Number: Input the prefix number of PLC Cnet Module.
- 32bit Data Swap: 32bit can be expressed in the combination of [Upper level word + Lower level word] or [Lower level word + Upper level word] and for this, it is available to use swap of upper level word and lower level word.
- Save: If 'Save' button is pressed, Station information will be saved and the saved information will add to the left "Configuration Information" tree.



(3) Add Block



- Select [New Block] from “Configuration Information” tree.
- Block Number: This number is a unique code of the block. The user needs to designate a different code to each block.
- Description: Input some information on the block.
- Start Address: Input the Block’s Start Address. There are four kinds and each address is designated as the following ways respectively:
 - Address delimiter 0(Coil Status), 1(Discrete Input Status), 3(Input Register), 4(Holding Register)
 - Its address is 0~65536 and if “Start Offset Address” is set up to start from 1 in the configuration information, it will be 1~65536
- Period: Input an interval to collect data of the relevant block (unit: msec).
- Count: A number to read for each corresponding delimiter.
- Save: If ‘Save’ button is pressed, Block information will be saved and the saved information will add to the left “Configuration Information” tree.
- Delete: If “Delete” button is pressed, the currently selected Block will be deleted.



(4) I/O Address

1) Analog

Delimiter (3 or 4) +0~65535

(if "Start Offset Address" is set up to start from 1 in the configuration information , it will be 1~65536)

Example 1) If the user wants to read 0th(0 of 0~65535) of No. 3 (Input Register: Read only),

Set up 300000 or 30 if 0 is selected for "Start Offset Address"

Set up 300001 or 31 if 1 is selected for "Start Offset Address"

Example 2) If the user wants to read 17th(17 of 0~65535) of No. 4 (Holding Register),

Set up 400017 or 417 if 0 is selected for "Start Offset Address"

Set up 400018 or 418 if 1 is selected for "Start Offset Address"

2) Digital

Delimiter (0 or 1, or 3 or 4) +0~65535

(if "Start Offset Address" is set up to start from 1 in the configuration information , it will be 1~65536)

Example 1) If the user wants to read 0th(0 of 0~65535) of No. 0 (Coil Status : Read/Write),

Set up 000000 or 00 if 0 is selected for "Start Offset Address"

Set up 000001 or 01 if 1 is selected for "Start Offset Address"

Example 2) If the user wants to read 17th(17 of 0~65535) of No. 1 (Discrete Input Status: Read only),

Set up 100017 or 117 if 0 is selected for "Start Offset Address"

Set up 100018 or 118 if 1 is selected for "Start Offset Address"

Example 3) If the user wants to read 10th bit of 17th(17 of 0~65535) of No. 3 (Input Register: Read only),

Set up 300017.A or 317.A if 0 is selected for "Start Offset Address"

Set up 300018.A or 318.A if 1 is selected for "Start Offset Address"

Example 4) If the user wants to read 15th bit of 0th(0 of 0~65535) of No. 4 (Holding Register),

Set up 300000.F or 30.F if 0 is selected for "Start Offset Address"

Set up 300001.F or 31.F if 1 is selected for "Start Offset Address"

15.4 Available Device

The available device for InfoU is as below.

Device	Area allowed for connection			Remarks
	Available range	Reading (function code)	Writing (function code)	
Output contacts	0 - 65535	Available (01)	Available (05)	-
Input contacts	0 - 65535	Available (02)	Available (05)	-
Output register	0 - 65535	Available (03)	Available (06,16)	-
Input register	0 - 65535	Available (04)	Available (06,16)	-

Notice

- For the details on device, refer to MODBUS Protocol manual of Schneider.
- Use it within device area.
- The maximum device value may be different depending on PLC so refer to the PLC manual to be connected.