FnIO S–Series: NA-9289

MODBUS/TCP(UDP) Adapter

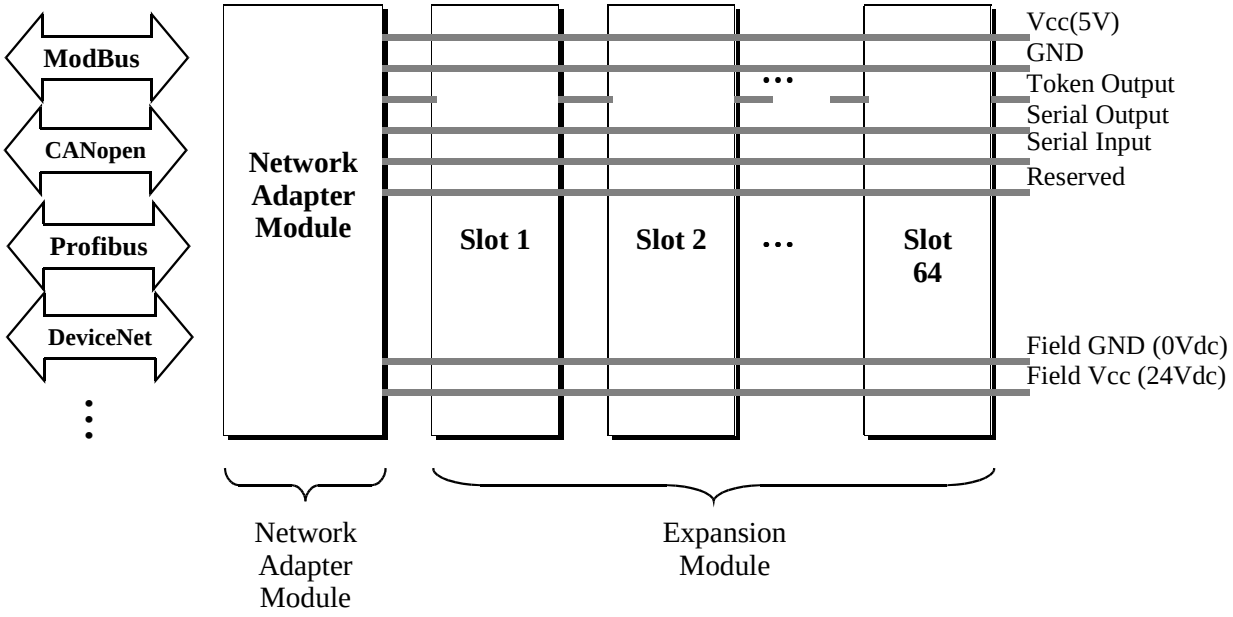
with Two RJ-45

DOCUMENT CHANGE SUMMARY				
REV.	**PAGES**	**REMARKS**	**DATE**	**Editor**
Released			May.2 1, 2013	Crevis

Table of Contents

1. FNBUS OVERVIEW

1.1. FnBus System

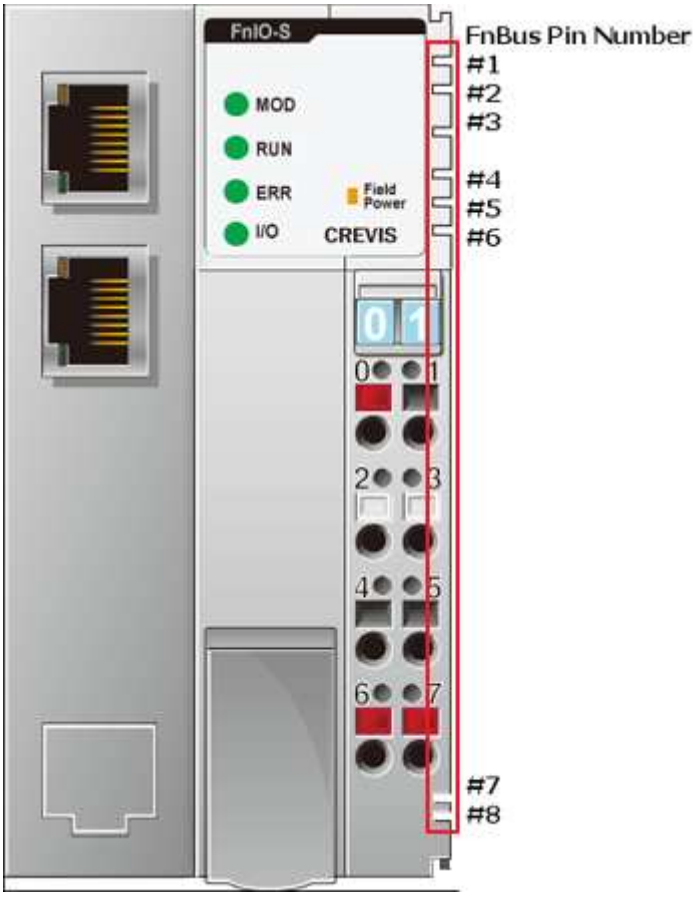


Network Adapter Module
The Network Adapter Module forms the link between the fieldbus and the field devices with the Expansion Modules. The connection to different fieldbus systems can be established by each of the corresponding Network Adapter Module, e.g. for SynqNet, PROFIBUS, CANopen, DeviceNet , Ethernet/IP, CC-Link, MODBUS/Serial, MODBUS/TCP etc.

Expansion Module
The Expansion Modules are supported a variety of input and output field devices.
There are digital and analog input/output modules and special function modules.

Two types of FnBus Message
- Service Messaging
- I/O Messaging

1.2. FnBus Pin Description

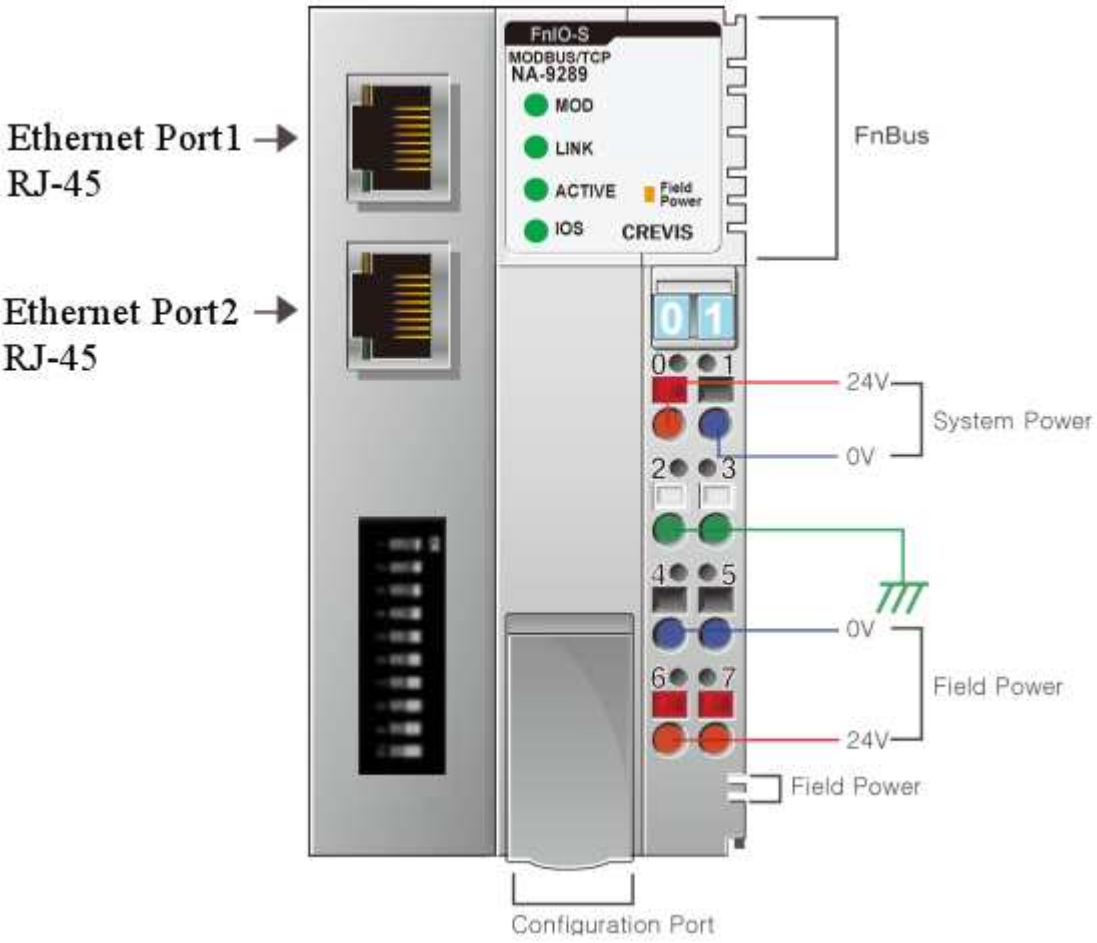


No.	Name	Description
1	Vcc	System supply voltage (5V dc).
2	GND	System Ground.
3	Token Output	Token output port of Processor module.
4	Serial Output	Transmitter output port of Processor module.
5	Serial Input	Receiver input port of Processor module.
6	Reserved	Reserved for bypass Token.
7	Field GND	Field Ground.
8	Field Vcc	Field supply voltage (24Vdc).

2. MODBUS/TCP ADAPTER MODULE

2.1. Shape

NA-9289, MODBUS/TCP(UDP)



POWER Connector Signal Assignment

Pin No.	Description	Pin No.	Description
0	System Power, 24V	1	System Power, Ground
2	FG	3	FG
4	Field Power, Ground	5	Field Power, Ground
6	Field Power, 24V	7	Field Power, 24V

2.2. MODBUS/TCP Adapter Specification

■ **Specification**

Interface Specification, NA-9289(MODBUS/TCP)	
Adapter Type	Slave node (MODBUS/TCP, MODBUS/UDP Server)
Max. Expansion Module	63 slots
Max. Input Size	252bytes
Max. Output Size	252bytes
Max. Length Bus Line	Up to100m from Ethernet Hub/Switch with twisted CAT 3 UTP/STP
Max. Nodes	Limited by Ethernet Specification.
Baud rate	10/100Mbps, Auto-negotiation, Full duplex
Protocol	MODBUS/TCP, MODBUS/UDP, DHCP 10 TCP Connections
Interface Connector	RJ-45 socket * 2pcs
IP-Address Setup	Via DHCP or IOGuide(Crevis Configuration Software)
Serial Configuration (RS232)	Node : 1 (Fixed) Baud Rate : 115200 (Fixed) Data bit : 8 (Fixed) Parity bit : No parity (Fixed) Stop bit : 1 (Fixed)
Indicator	5 LEDs 1 Green/Red, Module Status (MOD) 1 Green, Physical Connection (LINK) 1 Green, Exchange Data/Traffic Present (ACTIVE) 1 Green/Red Expansion Module Status (IOS) 1 Green, Field Power Status
Module Location	Starter module – left side of FnIO system
Field Power Detection	About 11Vdc
General Specification	
System Power	Supply voltage : 24Vdc nominal Supply voltage range : 11~28.8Vdc Protection : Output current limit(Min. 1.5A) Reverse polarity protection
Power Dissipation	100mA typical @24Vdc
Current for I/O Module	1.5A @5Vdc
Isolation	System power to internal logic : Non-isolation System power to I/O driver : Isolation
Field Power	Supply voltage : 24Vdc nominal Supply voltage range : 11~28.8Vdc
Max. Current Field Power Contact	DC 10A Max.
Weight	167g
Module Size	54mm x 99mm x 70mm
Environment Condition	Refer to Environment Specification

2.3. LED Indicator

2.3.1. Module Status LED (MOD)

State	LED is:	To indicate:
No Power	Off	No power is supplied to the unit.
Device Operational	Green	The unit is operating in normal condition.
Device in Standby	Flashing Green	The device needs commissioning due to configuration missing, incomplete or incorrect.
MODBUS Error	Green/Red Toggle	MODBUS error such as watchdog error, etc.
Minor Fault	Flashing Red	Recoverable Fault - EEPROM sum check error.
Unrecoverable Fault	Red	The device has an unrecoverable fault. - Memory error or CPU watchdog error.

2.3.2. Physical Connection LED (LINK)

State	LED is :	To indicate :
Not Powered or Not Linked	Off	Device may not be powered
Adapter physical connected	Green	Adapter Ethernet Controller physically connected.

2.3.3. Exchange Data/Traffic Present LED (ACTIVE)

State	LED is :	To indicate :
Not Powered	Off	Device is idle or may not be powered
Adapter exchange data	Green Flashing	Adapter(Slave) exchange data/Traffic present. About 10msec flashing.

2.3.4. Expansion IO Module Status LED (IOS)

State	LED is :	To indicate :
Not Powered No Expansion Module	Off	Device has no expansion module or may not be powered
FnBus On-line, Do not Exchanging I/O	Flashing Green	FnBus is normal but does not exchanging I/O data (Passed the expansion module configuration).
FnBus Connection, Run Exchanging IO	Green	Exchanging I/O data
Expansion Configuration Failed	Flashing Red	Failed to initialize expansion module - Detected invalid expansion module ID. - Overflowed Input/Output Size - Too many expansion module - Initial protocol failure - Mismatch vendor code between adapter and expansion module.
FnBus connection fault during exchanging IO	Red	One or more expansion module occurred in fault state. - Changed expansion module configuration. - FnBus communication failure.

2.3.5. Field Power Status LED

State	LED is :	To indicate :
Not Supplied Field Power	Off	Not supplied 24V dc field power
Supplied Field Power	Green	Supplied 24V dc field power

2.3.6. RJ-45, Electrical Interface

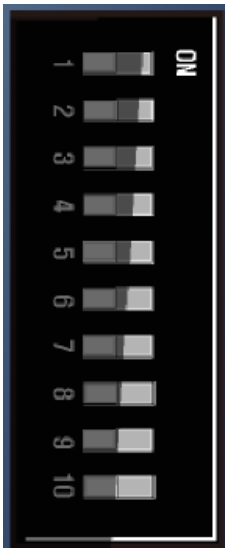
Shielded RJ-45 Socket

PORT1

RJ-45	Signal Name	Description
1	TD+	Transmit +
2	TD-	Transmit +
3	RD+	Receive +
4	----	
5	----	
6	RD-	Receive -
7	----	
8	----	
Case	Shield	

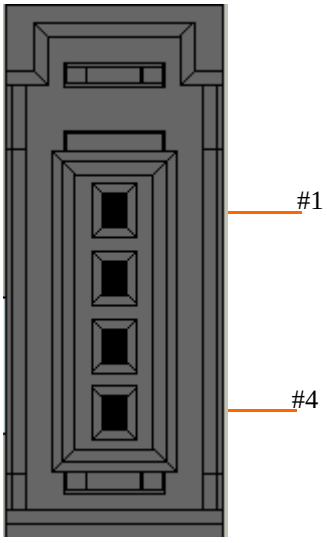
PORT2

2.3.7. DIP Switch



DIP Pole#	Description	
1	IP_DIP bit#0	Lowest IP Address when Pole#10=ON, then IP Address will be XXX.XXX.XXX.IP_DIP
2	IP_DIP bit#1	
3	IP_DIP bit#2	
4	IP_DIP bit#3	
5	IP_DIP bit#4	
6	IP_DIP bit#5	
7	IP_DIP bit#6	
8	IP_DIP bit#7	
9	=ON : Enable DHCP	
10	=ON : Use Lowest IP Address with IP_DIP value	

2.3.8. RS232 Port for MODBUS/RTU, Touch Panel or IOGuide



RS232 (37204-62A3-004PL/3M)

Pin#	Signal Name	Description
1	Reserved	----
2	TXD	RS232 TXD
3	RXD	RS232 RXD
4	GND	RS232 Ground

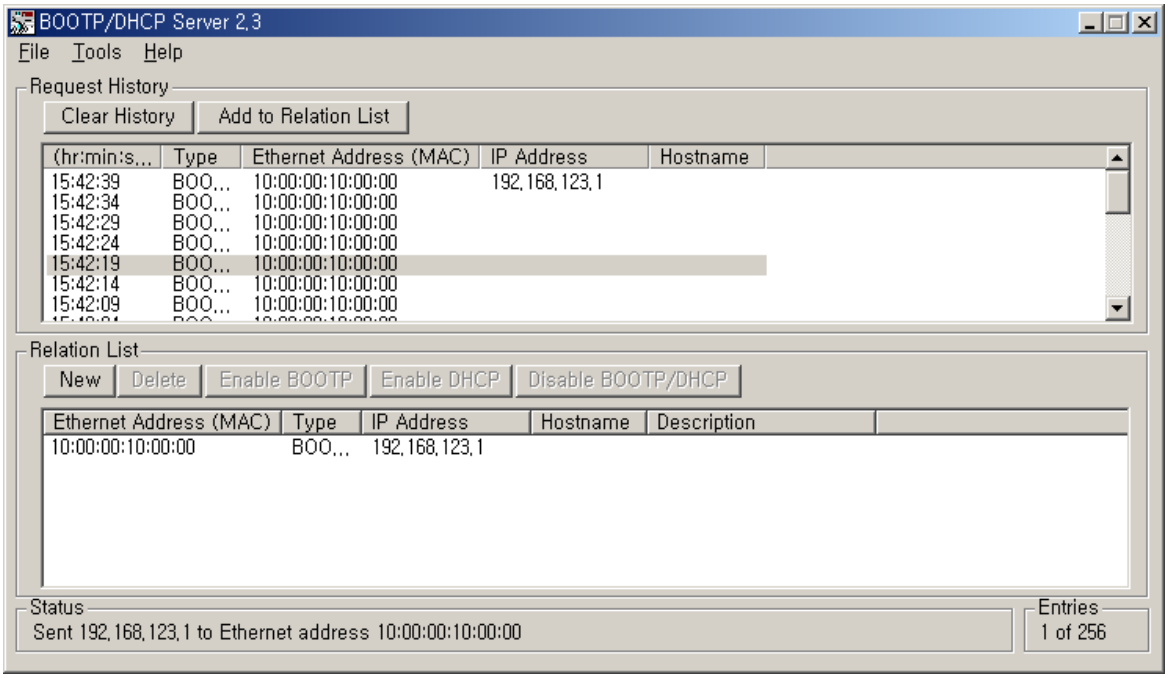
2.4. MODBUS/TCP IP-Address Setup

2.4.1. IP-Address Setup using DHCP Server

If the adapter DHCP enabled (DIP Pole#9 ON), the adapter sends DHCP request message of 20 times every 5sec. If DHCP sever does not response, the Adapter applies its IP Address with EEPROM (Latest saved IP Address).

The following is an example of adapter IP-Address setup that can be used with a third party BOOTP/DHCP server.

- ex) Rockwell Automation' s BOOTP/DHCP server

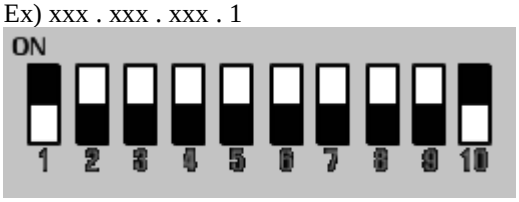


2.4.2. IP-Address Setup using Dip Switch(Manual Function)

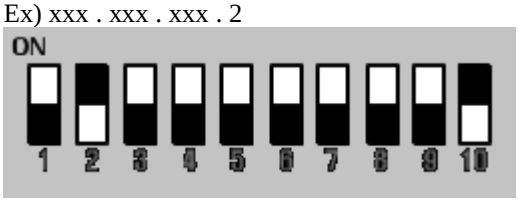
If the adapter DIP Pole#10 is ON, lowest IP address is set by DIP Pole#1~#8 manually. Refer to 2.3.7.

These are examples of adapter IP-Address setup by manual function.

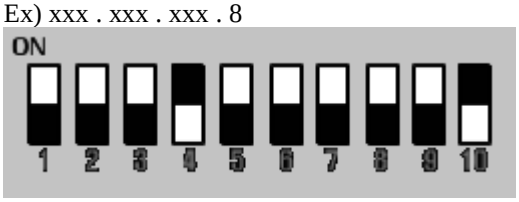
Ex) xxx . xxx . xxx . 1



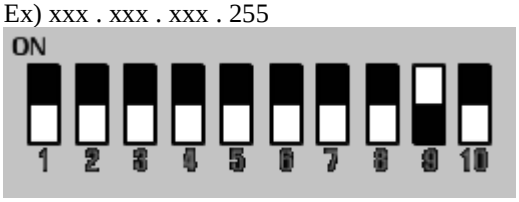
Ex) xxx . xxx . xxx . 2



Ex) xxx . xxx . xxx . 8



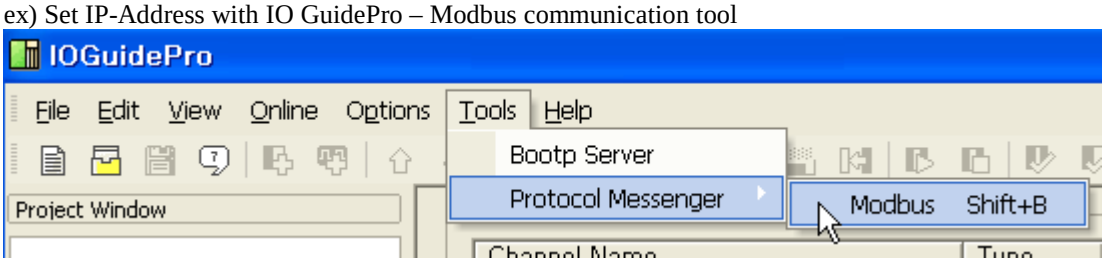
Ex) xxx . xxx . xxx . 255

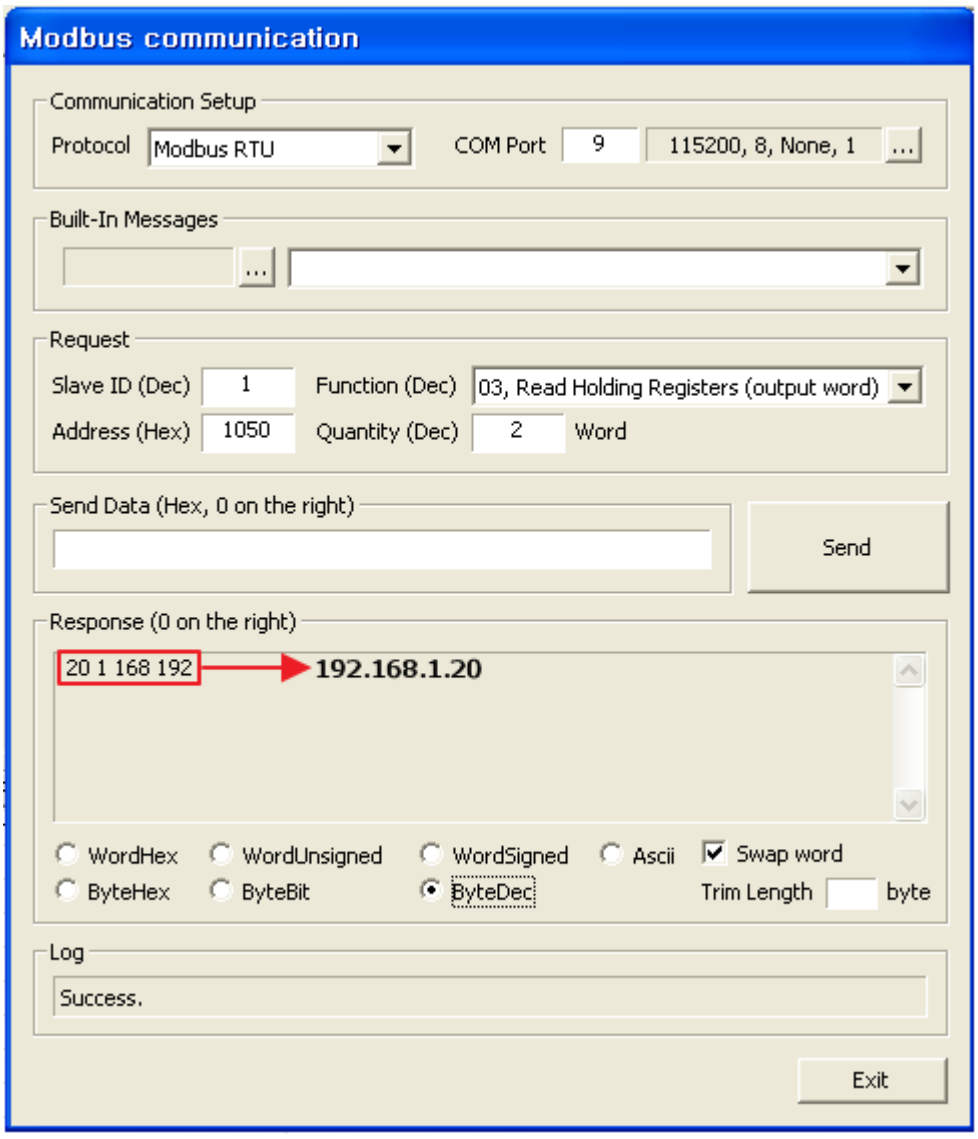


2.4.3. IP-Address Setup using Adapter TCP/IP Special Register

IP-Address can be set by adapter TCP/IP special register 0x1050(4176). Refer to 3.3.3.

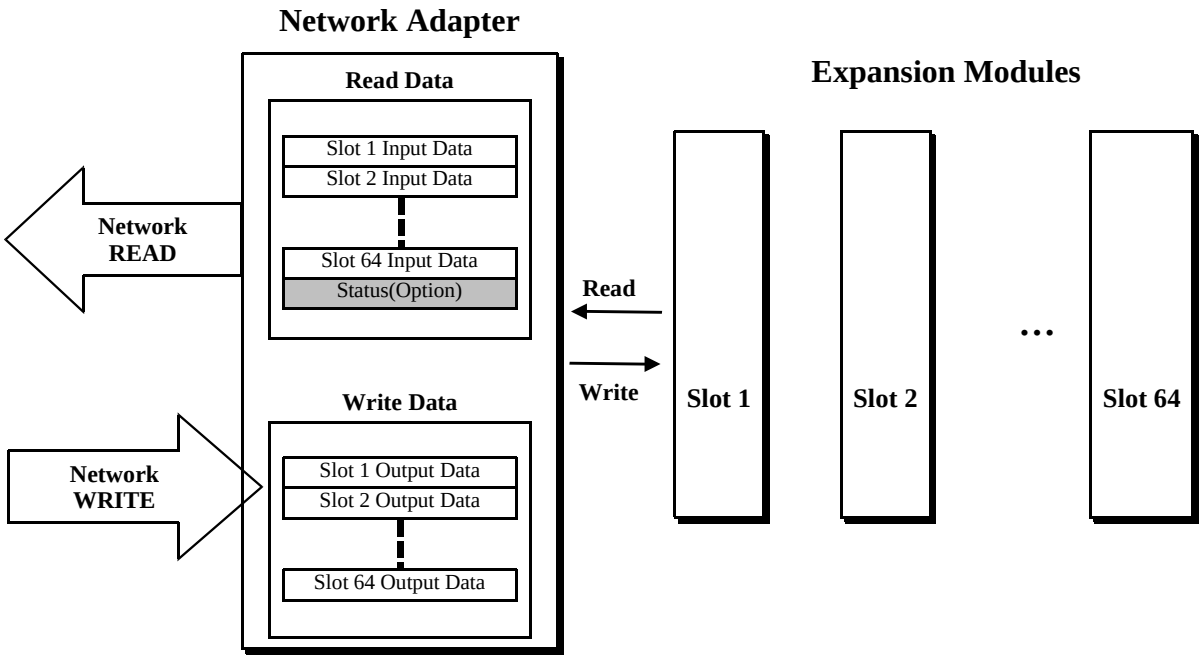
ex) Set IP-Address with IO GuidePro – Modbus communication tool





2.5. I/O Process Image Map

An expansion module may have 3 types of data as I/O data, configuration parameter and memory register.
The data exchange between network adapter and expansion modules is done via an I/O process image data by FnBus protocol. The following figure shows the data flow of process image between network adapter and expansion modules.



2.5.1. MODBUS Interface Register/Bit Map

■ **Register Map**

Start Address	Read/Write	Description	Func. Code
0x0000 ~	Read	Process input image registers (Real Input Register)	4,23
0x0800 ~	Read/Write	Process output image registers (Real Output Register)	3,16,23
0x1000 *	Read	Adapter Identification special registers.	3,4,23
0x1020 *	Read/Write	Adapter Watchdog, other time special register.	3,4,6,16,23
0x1100 *	Read/Write	Adapter Information special registers.	3,4,6,16,23
0x2000 *	Read/Write	Expansion Slot Information special registers.	3,4,6,16,23
Start Address	**Read/Write**	**Description**	

* The special register map must be accessed by read/write of every each address (one address).

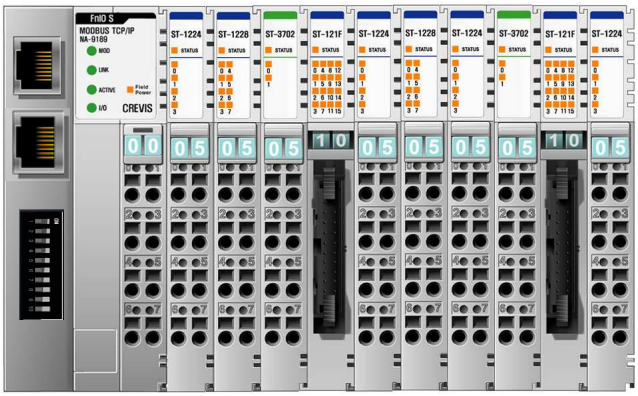
■ **Bit Map**

Start Address	Read/Write	Description	Func. Code
0x0000~	Read	Process input image bits All input registers area are addressable by bit address. Size of input image bit is size of input image register * 16.	2
0x1000~	Read/Write	Process output image bits All output registers area are addressable by bit address. Size of output image bit is size of output image register * 16.	1,5,15

2.5.2. Example of Input Process Image(Input Register) Map

Input image data depends on slot position and expansion slot data type. Input process image data is only ordered by expansion slot position when input image mode is uncompressed (mode 0, 2). But, when input image mode is compressed (mode 1, 3), input process image data is ordered by expansion slot position and slot data type.
Input process image mode can be set by special register 0x1114(4372). Refer to 3.3.3.

- **For example slot configuration**



Slot Address	Module Description
#0	MODBUS Adapter
#1	4-discrete input
#2	8-discrete input
#3	2-analog input
#4	16-discrete input
#5	4-discrete input
#6	8-discrete input
#7	4-discrete input
#8	2-analog input
#9	16-discrete input
#10	4-discrete input

Status (1word)

- **Input Process Image Mode#0** (Status(1word) + Uncompressed Input Processing Data)

Addr.	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
0x0000	EW	0	0	0	0	0	0	0	FP	FnBus Status						
0x0001	Discrete In 8pts (Slot#2)								Empty, Always 0				Discrete In 4pts (Slot#1)			
0x0002	Analog Input Ch0 high byte (Slot#3)								Analog Input Ch0 low byte (Slot#3)							
0x0003	Analog Input Ch1 high byte (Slot#3)								Analog Input Ch1 low byte (Slot#3)							
0x0004	Discrete In high 8pts (Slot#4)								Discrete In low 8pts (Slot#4)							
0x0005	Discrete In 8pts (Slot#6)								Empty, Always 0				Discrete In 4pts (Slot#5)			
0x0006	Analog Input Ch0 low byte (Slot#8)								Empty, Always 0				Discrete In 4pts (Slot#7)			
0x0007	Analog Input Ch1 low byte (Slot#8)								Analog Input Ch0 high byte (Slot#8)							
0x0008	Discrete In low 8pts (Slot#9)								Analog Input Ch1 high byte (Slot#8)							
0x0009	Empty, Always 0					Discrete In 4pts (Slot#10)			Discrete In high 8pts (Slot#9)							

- FnBus Status:
  0: Normal Operation
  1: FnBus Standby
  2: FnBus Communication Fault
  3: Slot Configuration Failed
  4: No Expansion Slot
- FP (Field Power)
  0: 24Vdc Field Power On.
  1: 24Vdc Field Power Off
- EW (MODBUS Error Watchdog)
  0: No Error Watchdog
  1: Error Watchdog once more since its last restart, clear counters operation, or power-up.

Status (1word)

■ **Input Process Image Mode#1** (Status(1word) + Compressed Input Processing Data)

Addr.	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
0x0000	EW	0	0	0	0	0	0	0	FP	FnBus Status						
0x0001	Analog Input Ch0 high byte (Slot#3)								Analog Input Ch0 low byte (Slot#3)							
0x0002	Analog Input Ch1 high byte (Slot#3)								Analog Input Ch1 low byte (Slot#3)							
0x0003	Analog Input Ch0 high byte (Slot#8)								Analog Input Ch0 low byte (Slot#8)							
0x0004	Analog Input Ch1 high byte (Slot#8)								Analog Input Ch1 low byte (Slot#8)							
0x0005	Discrete In low 8pts (Slot#4)								Discrete In 8pts (Slot#2)							
0x0006	Discrete In 8pts (Slot#6)								Discrete In high 8pts (Slot#4)							
0x0007	Discrete In high 8pts (Slot#9)								Discrete In low 8pts (Slot#9)							
0x0008	Discrete In 4pts (Slot#10)				Discrete In 4pts (Slot#7)				Discrete In 4pts (Slot#5)				Discrete In 4pts (Slot#1)			

- Input Assembly Priority:
  1) Analog Input Data (Word type)
  2) 8 or 16 points Discrete Input Data (Byte type)
  3) 4 points Input Data (Bit type)
  4) 2 points Input Data (Bit type)

■ **Input Process Image Mode#2** (Uncompressed Input Processing Data without Status), **default input image**

Addr.	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
0x0000	Discrete In 8pts (Slot#2)								Always 0				Discrete In 4pts (Slot#1)			
0x0001	Analog Input Ch0 high byte (Slot#3)								Analog Input Ch0 low byte (Slot#3)							
0x0002	Analog Input Ch1 high byte (Slot#3)								Analog Input Ch1 low byte (Slot#3)							
0x0003	Discrete In high 8pts (Slot#4)								Discrete In low 8pts (Slot#4)							
0x0004	Discrete In 8pts (Slot#6)								Empty, Always 0				Discrete In 4pts (Slot#5)			
0x0005	Analog Input Ch0 low byte (Slot#8)								Empty, Always 0				Discrete In 4pts (Slot#7)			
0x0006	Analog Input Ch1 low byte (Slot#8)								Analog Input Ch0 high byte (Slot#8)							
0x0007	Discrete In low 8pts (Slot#9)								Analog Input Ch1 high byte (Slot#8)							
0x0008	Empty, Always 0				Discrete In 4pts (Slot#10)				Discrete In high 8pts (Slot#9)							

■ **Input Process Image Mode#3** (Compressed Input Processing Data without Status)

Addr.	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
0x0000	Analog Input Ch0 high byte (Slot#3)								Analog Input Ch0 low byte (Slot#3)							
0x0001	Analog Input Ch1 high byte (Slot#3)								Analog Input Ch1 low byte (Slot#3)							
0x0002	Analog Input Ch0 high byte (Slot#8)								Analog Input Ch0 low byte (Slot#8)							
0x0003	Analog Input Ch1 high byte (Slot#8)								Analog Input Ch1 low byte (Slot#8)							
0x0004	Discrete In low 8pts (Slot#4)								Discrete In 8pts (Slot#2)							
0x0005	Discrete In 8pts (Slot#6)								Discrete In high 8pts (Slot#4)							
0x0006	Discrete In high 8pts (Slot#9)								Discrete In low 8pts (Slot#9)							
0x0007	Discrete In 4pts (Slot#10)				Discrete In 4pts (Slot#7)				Discrete In 4pts (Slot#5)				Discrete In 4pts (Slot#1)			

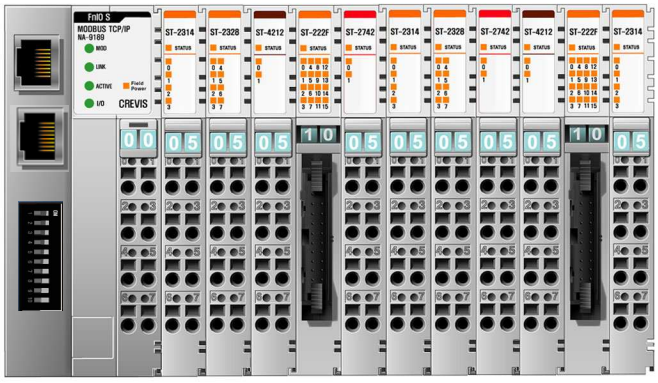
* FnBus uses the byte-oriented register mapping.
* Size of input image bit is size of input image register * 16.

- Input Assembly Priority:
  1) Analog Input Data (Word type)
  2) 8 or 16 points Discrete Input Data (Byte type)
  3) 4 points Input Data (Bit type)
  4) 2 points Input Data (Bit type)

2.5.3. Example of Output Process Image(Output Register) Map

Output image data depends on slot position and expansion slot data type. Output process image data is only ordered by expansion slot position when output image mode is uncompressed (mode 0). But, when output image mode is compressed (mode 1), output process image data is ordered by expansion slot position and slot data type.
Output process image mode can be set by special register 0x1115(4373). Refer to 3.3.3.

- **For example slot configuration**



Slot Address	Module Description
#0	MODBUS Adapter
#1	4-discrete output
#2	8-discrete output
#3	2-analog output
#4	16-discrete output
#5	4-discrete output
#6	8-discrete output
#7	2-realy output
#8	2-realy output
#9	2-analog output
#10	16-discrete output
#11	4-discrete output

- **Output Process Image Mode#0** (Uncompressed Output Processing Data), **default output image**

Addr.	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
0x0800	Discrete Out 8pts (Slot#2)								Empty, Don't care				Discrete Out 4pts(Slot#1)			
0x0801	Analog Output Ch0 high byte (Slot#3)								Analog Output Ch0 low byte (Slot#3)							
0x0802	Analog Output Ch1 high byte (Slot#3)								Analog Output Ch1 low byte (Slot#3)							
0x0803	Discrete Out high 8pts (Slot#4)								Discrete Out low 8pts (Slot#4)							
0x0804	Discrete Out 8pts (Slot#6)								Empty, Don't care				Discrete Out 4pts(Slot#5)			
0x0805	Empty, Don't care						Discrete Out 2pts (Slot#8)		Empty, Don't care						Discrete Out 2pts (Slot#7)	
0x0806	Analog Output Ch0 high byte (Slot#9)								Analog Output Ch0 low byte (Slot#9)							
0x0807	Analog Output Ch1 high byte (Slot#9)								Analog Output Ch1 low byte (Slot#9)							
0x0808	Discrete Output high 8pts (Slot#10)								Discrete Output low 8pts (Slot#10)							
0x0809	Empty, Don't care								Empty, Don't care				Discrete Out 4pts(Slot#11)			

- **Output Process Image Mode#1** (Compressed Output Processing Data)

Addr.	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
0x0800	Analog Output Ch0 high byte (Slot#3)								Analog Output Ch0 low byte (Slot#3)							
0x0801	Analog Output Ch1 high byte (Slot#3)								Analog Output Ch1 low byte (Slot#3)							
0x0802	Analog Output Ch0 high byte (Slot#9)								Analog Output Ch0 low byte (Slot#9)							
0x0803	Analog Output Ch1 high byte (Slot#9)								Analog Output Ch1 low byte (Slot#9)							
0x0804	Discrete Output low 8 pts (Slot#4)								Discrete Out 8pts (Slot#2)							
0x0805	Discrete Out 8pts (Slot#6)								Discrete Out high 8pts (Slot#4)							
0x0806	Discrete Out high 8pts (Slot#10)								Discrete Out low 8pts (Slot#10)							
0x0807	Discrete Out 2pts (Slot#8)				Discrete Out 2pts (Slot#7)				Discrete Out 4pts (Slot#11)				Discrete Out 4pts (Slot#5)		Discrete Out 4pts (Slot#1)	

* FnBus uses the byte-oriented register mapping.
* Size of output image bit is size of output image register * 16.

- Output Assembly Priority:
  1) Analog Output Data (Word type)
  2) 8 or 16 points Discrete Output Data (Byte type)
  3) 4 points Output Data (Bit type)
  4) 2 points Output Data (Bit type)

3. MODBUS/TCP INTERFACE

3.1. MODBUS/TCP, UDP Protocol

The MODBUS messaging service provides a Client/Server communication between devices connected on an Ethernet TCP/IP network. All MODBUS/TCP or MODBUS/UDP messages are sent via TCP(UDP) on registered port 502. Refer to Modbus_Messaging_Implementation_Guide_V1_0a.pdf.

3.1.1. Comparison of MODBUS/TCP, MODBUS/UDP And MODUB/RTU

This header provides some differences compared to the MODBUS RTU application data unit used on serial line:
• The MODBUS ‘slave address’ field usually used on MODBUS Serial Line is replaced by a single byte ‘Unit Identifier’ within the MBAP Header. The ‘Unit Identifier’ is used to communicate via devices such as bridges, routers and gateways that use a single IP address to support multiple independent MODBUS end units.
• All MODBUS requests and responses are designed in such a way that the recipient can verify that a message is finished. For function codes where the MODBUS PDU has a fixed length, the function code alone is sufficient. For function codes carrying a variable amount of data in the request or response, the data field includes a byte count.
• When MODBUS is carried over TCP, additional length information is carried in the MBAP header to allow the recipient to recognize message boundaries even if the message has been split into multiple packets for transmission. The existence of explicit and implicit length rules, and use of a CRC-32 error check code (on Ethernet) results in an infinitesimal chance of undetected corruption to a request or response message.

MODBUS/TCP

MBAP Header	Function	Data
7 chars	1 char	Up to 252 chars

MODBUS/RTU

Start	Address	Function	Data	CRC Check	End
≥ 3.5 char	1 char	1 char	Up to 252 chars	2 chars	≥ 3.5 char

Function and data field of MODBUS/TCP are identical to function and data field of MODBUS/RTU.

3.1.2. MODBUS/TCP, MODBUS/UDP MBAP Header

The MBAP (MODBUS Application Protocol) header contains the following fields.

Fields	Length	Description	Client	Server
Transaction Identifier	2byes	Identification of a MODBUS Request /Response transaction.	Initialized by the client	Recopied by the server from the received
Protocol Identifier	2bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received
Length	2bytes	Number of following bytes	Initialized by the client (Request)	Initialized by the server (Response)
Unit Identifier	1byte	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the client	Recopied by the server from the received

• Transaction Identifier - It is used for transaction pairing, the MODBUS server copies in the response the transaction identifier of the request.
• Protocol Identifier – It is used for intra-system multiplexing. The MODBUS protocol is identified by the value 0.

• Length - The length field is a byte count of the following fields, including the Unit Identifier and data fields.
• Unit Identifier – This field is used for intra-system routing purpose. Typically MODBUS server must be returned with the same value set by MODBUS client.

3.2. Supported MODBUS Function Codes

Function Code	Function	Description
1(0x01)	Read Coils	Read output bit
2(0x02)	Read Discrete Inputs	Read input bit
3(0x03)	Read Holding Registers	Read output word
4(0x04)	Read Input Registers	Read input word
5(0x05)	Write Single Coil	Write one bit output
6(0x06)	Write Single Register	Write one word output
8(0x08)	Diagnostics	Read diagnostic register
15(0x0F)	Write Multiple Coils	Write a number of output bits
16(0x10)	Write Multiple registers	Write a number of output words
23(0x17)	Read/Write Multiple registers	Read a number of input words /Write a number of output words

- Refer to MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1a

3.2.1. 1 (0x01) Read Coils

This function code is used to read from 1 to 2000 contiguous status of coils in a remote device. The Request PDU specifies the starting address, i.e. the address of the first coil specified, and the number of coils. In the PDU Coils are addressed starting at zero. Therefore coils numbered 1-16 are addressed as 0-15. The coils in the response message are packed as one coil per bit of the data field. Status is indicated as 1= ON and 0= OFF.

■ **Request**

Field name	Example
Function Code	0x01
Starting Address Hi	0x10
Starting Address Lo	0x00
Quantity of Outputs Hi	0x00
Quantity of Outputs Lo	0x0A

■ **Response**

Field name	Example
Function Code	0x01
Byte Count	0x02
Output Status	0x55
Output Status	0x02

- In case of address 0x1015~0x1000 output bit value: 10101010_01010101.

3.2.2. 2 (0x02) Read Discrete Inputs

This function code is used to read from 1 to 2000 contiguous status of discrete inputs in a remote device. The Request PDU specifies the starting address, i.e. the address of the first input specified, and the number of inputs. In the PDU Discrete Inputs are addressed starting at zero. Therefore Discrete inputs numbered 1-16 are addressed as 0-15.

The discrete inputs in the response message are packed as one input per bit of the data field.
Status is indicated as 1= ON; 0= OFF.

■ **Request**

Field name	Example
Function Code	0x02
Starting Address Hi	0x00
Starting Address Lo	0x00
Quantity of Inputs Hi	0x00
Quantity of Inputs Lo	0x0A

■ **Response**

Field name	Example
Function Code	0x02
Byte Count	0x02
Input Status	0x80
Input Status	0x00

- In case of address 0x0015~0x0000 input bit value: 00000000_10000000.

3.2.3. 3 (0x03) Read Holding Registers

This function code is used to read the contents of a contiguous block of holding registers in a remote device. The Request PDU specifies the starting register address and the number of registers.
The register data in the response message are packed as two bytes per register, with the binary contents right justified within each byte. For each register, the first byte contains the high order bits and the second contains the low order bits.

■ **Request**

Field name	Example
Function Code	0x03
Starting Address Hi	0x08
Starting Address Lo	0x00
Quantity of Register Hi	0x00
Quantity of Register Lo	0x02

■ **Response**

Field name	Example
Function Code	0x03
Byte Count	0x04
Output Register#0 Hi	0x11
Output Register#0 Lo	0x22
Output Register#1 Hi	0x33
Output Register#1 Lo	0x44

- In case of address 0x0800, 0x0801 output register value: 0x1122, 0x3344.

3.2.4. 4 (0x04) Read Input Registers

This function code is used to read from 1 to approx. 125 contiguous input registers in a remote device. The Request PDU specifies the starting register address and the number of registers. The register data in the response message are packed as two bytes per register, with the binary contents right justified within each byte. For each register, the first byte contains the high order bits and the second contains the low order bits.

■ **Request**

Field name	Example
Function Code	0x04
Starting Address Hi	0x00
Starting Address Lo	0x00
Quantity of Register Hi	0x00
Quantity of Register Lo	0x02

■ **Response**

Field name	Example
Function Code	0x03
Byte Count	0x04
Input Register#0 Hi	0x00
Input Register#0 Lo	0x80
Input Register#1 Hi	0x00
Input Register#1 Lo	0x00

- In case of address 0x0000, 0x0001 input register value: 0x0080, 0x0000.

3.2.5. 5 (0x05) Write Single Coil

This function code is used to write a single output to either ON or OFF in a remote device. The requested ON/OFF state is specified by a constant in the request data field. A value of FF 00 hex requests the output to be ON. A value of 00 00 requests it to be OFF. All other values are illegal and will not affect the output.

■ **Request**

Field name	Example
Function Code	0x05
Output Address Hi	0x10
Output Address Lo	0x01
Output Value Hi	0xFF
Output Value Lo	0x00

■ **Response**

Field name	Example
Function Code	0x05
Output Address Hi	0x10
Output Address Lo	0x01
Output Value Hi	0xFF
Output Value Lo	0x00

- Output bit of address 0x1001 turns ON.

3.2.6. 6 (0x06) Write Single Register

This function code is used to write a single holding register in a remote device. Therefore register numbered 1 is addressed as 0. The normal response is an echo of the request, returned after the register contents have been written.

■ **Request**

Field name	Example
Function Code	0x06
Register Address Hi	0x08
Register Address Lo	0x00
Register Value Hi	0x11

Register Value Lo	0x22

■ **Response**

Field name	Example
Function Code	0x06
Register Address Hi	0x08
Register Address Lo	0x00
Register Value Hi	0x11
Register Value Lo	0x22

- In case of address 0x0800 output register value: 0x0000 changes to 0x1122.

3.2.7. 8 (0x08) Diagnostics

MODBUS function code 08 provides a series of tests for checking the communication system between a client (Master) device and a server (Slave), or for checking various internal error conditions within a server.
The function uses a two–byte sub-function code field in the query to define the type of test to be performed. The server echoes both the function code and sub-function code in a normal response. Some of the diagnostics cause data to be returned from the remote device in the data field of a normal response.

■ **Request**

Field name	Example
Function Code	0x08
Sub-Function Hi	0x00
Sub-Function Lo	0x00
Data Hi	0x11
Data Lo	0x22

■ **Response**

Field name	Example
Function Code	0x08
Sub-Function Hi	0x00
Sub-Function Lo	0x00
Data Hi	0x11
Data Lo	0x22

Sub-function 0x0000(0) Return Query Data
The data passed in the request data field is to be returned (looped back) in the response.
The entire response message should be identical to the request.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0000(0)	Any	Echo Request Data	

Sub-function 0x0001(1) Restart Communications Option
The remote device could be initialized and restarted, and all of its communications event counters are cleared.
Especially, data field 0x55AA make the remote device to restart with factory default setup of EEPROM.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0001(1)	0x0000 or 0xFF00	Echo Request Data	Reset
0x0001(1)	0x55AA	Echo Request Data	Reset with Default Setting [1)]
0x0001(1)	0x55AA, 0xAB7B	Echo Request Data	Reset with Factory default [2)]

1),2) All expansion slot configuration parameters are cleared.
2) IP Address, Subnet Mask Address, Gateway Address will be the factory defaults value.

Sub-function 0x000A(10) Clear Counters and Diagnostic Register
The goal is to clear all counters and the diagnostic register. Counters are also cleared upon power–up.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x000A(10)	0x0000	Echo Request Data	

Sub-function 0x000B(11) Return Bus Message Count
The response data field returns the quantity of messages that the remote device has detected on the communications system since its last restart, clear counters operation, or power–up.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x000B(11)	0x0000	Total Message Count	

Sub-function 0x000D(13) Return Bus Exception Error Count
The response data field returns the quantity of MODBUS exception responses returned by the remote device since its last restart, clear counters operation, or power–up.
Exception responses are described and listed in section 3.2.11.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x000D(13)	0x0000	Exception Error Count	

Sub-function 0x000E(14) Return Slave Message Count
The response data field returns the quantity of messages addressed to the remote device, or broadcast, that the remote device has processed since its last restart, clear counters operation, or power–up.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x000E(14)	0x0000	Slave Message Count	

Sub-function 0x000F(15) Return Slave No Response Count
The response data field returns the quantity of messages addressed to the remote device for which it has returned no response (neither a normal response nor an exception response), since its last restart, clear counters operation, or power–up.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x000F(15)	0x0000	Slave No Response Count	

Sub-function 0x0064(100) Return Slave ModBus, FnBus Status
The response data field returns the status of ModBus and FnBus addressed to the remote device.
This status values are identical with status 1word of input process image. Refer to 2.4.2.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0064(100)	0x0000	ModBus, FnBus Status	Same as status 1word

Sub-function 0x0065(101) Return Slave Watchdog Error Count
The response data field returns the quantity of watchdog error addressed to the remote device since its last restart, clear counters operation, or power–up.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0065(101)	0x0000	Watchdog Error Count	

Sub-function 0x0066(102) Change Slave IO Output Status
The sub-function with data fields is to clear watchdog counter and change IO output status. This may be used to simulate clear output and fault output.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0066(102)	0x0000	Echo Request Data	Ready output, automatically turns Normal output
0x0066(102)	0x0001, 0x0002, 0x0003	Echo Request Data	Clear output
0x0066(102)	0x0004	Echo Request Data	Normal output
0x0066(102)	0x0005, 0x0006, 0x0007	Echo Request Data	Fault output

3.2.8. 15 (0x0F) Write Multiple Coils

This function code is used to force each coil in a sequence of coils to either ON or OFF in a remote device. The Request

PDU specifies the coil references to be forced. Coils are addressed starting at zero. A logical '1' in a bit position of the field requests the corresponding output to be ON. A logical '0' requests it to be OFF.
The normal response returns the function code, starting address, and quantity of coils forced.

■ **Request**

Field name	Example
Function Code	0x0F
Starting Address Hi	0x10
Starting Address Lo	0x00
Quantity of Outputs Hi	0x00
Quantity of Outputs Lo	0x0A
Byte Count	0x02
Output Value#0	0x55
Output Value#1	0x01

■ **Response**

Field name	Example
Function Code	0x0F
Starting Address Hi	0x10
Starting Address Lo	0x00
Quantity of Outputs Hi	0x00
Quantity of Outputs Lo	0x0A

- In case of address 0x1015~0x1000 output bit value: 00000000_00000000 changes to 00000001_01010101.

3.2.9. 16 (0x10) Write Multiple registers

This function code is used to write a block of contiguous registers (1 to approx. 120 registers) in a remote device.
The requested written values are specified in the request data field. Data is packed as two bytes per register.
The normal response returns the function code, starting address, and quantity of registers written.

■ **Request**

Field name	Example
Function Code	0x0F
Starting Address Hi	0x10
Starting Address Lo	0x08
Quantity of Registers Hi	0x00
Quantity of Registers Lo	0x02
Byte Count	0x04
Register Value#0 Hi	0x11
Register Value#0 Lo	0x22
Register Value#1 Hi	0x33
Register Value#1 Lo	0x44

■ **Response**

Field name	Example
Function Code	0x0F
Starting Address Hi	0x10
Starting Address Lo	0x08
Quantity of Registers Hi	0x00
Quantity of Registers Lo	0x02

.- In case of address 0x0800, 0x0801 output register value: 0x0000, 0x0000 changes to 0x1122, 0x3344.

3.2.10. 23 (0x17) Read/Write Multiple registers

This function code performs a combination of one read operation and one write operation in a single MODBUS transaction. The write operation is performed before the read. The request specifies the starting address and number of holding registers to be read as well as the starting address, number of holding registers, and the data to be written. The byte count specifies the number of bytes to follow in the write data field.
The normal response contains the data from the group of registers that were read. The byte count field specifies the quantity of bytes to follow in the read data field.

■ **Request**

Field name	Example
Function Code	0x17
Read Starting Address Hi	0x08
Read Starting Address Lo	0x00
Quantity of Read Hi	0x00
Quantity of Read Lo	0x02
Write Starting Address Hi	0x08
Write Starting Address Lo	0x00
Quantity of Write Hi	0x00
Quantity of Write Lo	0x02
Byte Count	0x04
Write Reg. Value#0 Hi	0x11
Write Reg. Value#0 Lo	0x22
Write Reg. Value#1 Hi	0x33
Write Reg. Value#1 Lo	0x44

■ **Response**

Field name	Example
Function Code	0x17
Byte Count	0x04
Read Reg. Value#0 Hi	0x11
Read Reg. Value#0 Lo	0x22
Read Reg. Value#1 Hi	0x33
Read Reg. Value#1 Lo	0x44

- In case of address 0x0800, 0x0801 output register value: 0x0000, 0x0000 changes to 0x1122, 0x3344.

3.2.11. Error Response

In an exception response, the server sets the MSB of the function code to 1. This makes the function code value in an exception response exactly 80 hexadecimal higher than the value would be for a normal response.

■ **Exception Response Example**

Field name	Example
Function Code	0x81
Exception Code	0x02

■ **Exception Codes**

Exception Code	Name	Description
01	Illegal Function	The function code received in the query is not an allowable action for the server (or slave).
02	Illegal Data Address	The data address received in the query is not an allowable address for the server (or slave).

03	Illegal Data Value	A value contained in the query data field is not an allowable value for server (or slave).
04	Slave Device Failure	An unrecoverable error occurred while the server (or slave) was attempting to perform the requested action.
05	Acknowledge	The server (or slave) has accepted the request and is processing it, but a long duration of time will be required to do so.
06	Slave Device Busy	Specialized use in conjunction with programming commands. The server (or slave) is engaged in processing a long–duration program command. The client (or master) should retransmit the message later when the server (or slave) is free.
08	Memory Parity Error	The server (or slave) attempted to read record file, but detected a parity error in the memory. The client (or master) can retry the request, but service may be required on the server (or slave) device.
0A	Gateway Path Unavailable	Specialized use in conjunction with gateways, indicates that the gateway was unable to allocate an internal communication path from the input port to the output port for processing the request.

- NA-9289 response exception code 01, 02, 03, 04 and 06.

3.3. MODBUS Special Register Map

The special register map can be accessed by function code 3, 4, 6 and 16. Also the special register map must be accessed by read/write of every each address (one address).

3.3.1. Adapter Identification Special Register (0x1000, 4096)

Address	Access	Type, Size	Description
0x1000(4096)	Read	1word	Vendor ID = 0x02E5(741), Crevis. Co., Ltd.
0x1001(4097)	Read	1word	Device type = 0x000C, Network Adapter
0x1002(4098)	Read	1word	Product Code = 0x8040
0x1003(4099)	Read	1word	Firmware revision, if 0x0101, revision 1.01
0x1004(4100)	Read	2word	Product unique serial number
0x1005(4101)	Read	String upto 34byte	Product name string First 1word is length of valid character string Example) response as following "00 20 4E 41 2D 39 32 38 39 2C 4D 6F 64 62 75 73 2F 54 43 50 20 41 64 61 70 74 65 72 2C 46 6E 42 75 73" Valid character size = 0x0020 =32 characters "NA-9289,Modbus/TCP Adapter,FnBus"
0x1006(4102)	Read	1word	Sum check of EEPROM
0x1010(4112)	Read	2word	Firmware release date
0x1011(4113)	Read	2word	Product manufacturing inspection date
0x1012(4114)	Read	String upto 34byte	Vendor name string First 1word is length of valid character string.
0x101E(4126)	Read	15word	Composite Id of following address 0x1050(4176),0x1051(4177),0x1052(4178),0x1053(4179), 0x1000(4096),0x1001(4097),0x1002(4098),0x1003(4099),0x1004(4100)

- String Type consists of valid string length (first 1word) and array of characters

3.3.2. Adapter Watchdog Time, other Time Special Register (0x1020, 4128)

A watchdog timer can be configured for timeout periods up to 65535(1unit=100msec). The Watchdog timer will timeout (timer decreased, reached 0) if ModBus operation to the slave node does not occur over the configured watchdog value, then the slave adapter forces that slot output value is automatically set to user-configured fault actions and values.

Address	Access	Type, Size	Description
0x1020(4128)	Read/Write	1word	Watchdog time value 16bit unsigned. The time value is represented by multiples of 100msec. The 0 (watchdog timeout disabled) is default value. A changing of watchdog time value resets watchdog error and counter.
0x1021(4129)	Read	1word	Watchdog timer remain value This value is decreased every 100msec
0x1022(4130)	Read	1word	Watchdog error counter, it is cleared by writing address 0x1020
0x1023(4131)	Read/Write	1word	Enable/disable auto recovery Watchdog error when receiving new frame. 0:Disable, 1:Enable(default). Its value is stored in EEPROM.
0x1028(4136)	Read	2word	IO update time, main loop time. (100usec unit)

3.3.3. Adapter TCP/IP Special Register (0x1040, 4160).

Address	Access	Type, Size	Description
0x1040(4160)	Read	1word	MODBUS/TCP statistics. Same as input process image's status(1word). Hi byte is ModBus status, low byte is FnBus status. Refer to 2.4.2
0x1041(4161)	Read/Write TBD	1word	MODBUS/TCP connection timeout time. (0.5sec unit) Maximum time of ModBus connection to stay to be opened without receiving a ModBus request. 0~3600 The 120 (60sec) is default value. The value 0 disables connection time out specially.
0x1042(4162)	Read	1word	Number of ModBus/TCP connected, TBD
0x1043(4163)	Read	1word	ModBus/TCP(UDP) port, fixed 502
0x1044(4164)	Read	1word	Ethernet Interface Speed, 10(10Mbps) or 100(100Mbps)
0x1045(4165)	---	---	
0x1046(4166)	---	---	
0x1047(4167)	Read	1word	Enable/disable IP address setup using DHCP, 1:Enabled
0x1048(4168)	Read	1word	Enable/disable Lowest IP address via DIP Switch, 1:Enabled
0x1050(4176)	Read/Write*	2word	IP address. If 192.168.123.1, then 0xA8C0, 0x017B. After update this value, IP address, Subnet mask and Gateway are applied as new one.
0x1051(4177)	Read/Write*	2word	Subnet mask. If 255.255.255.0, then 0xFFFF, 0x00FF.
0x1052(4178)	Read/Write*	2word	Gateway. If 192.168.123.254, then 0xA8C0, 0xFE7B.
0x1053(4179)	Read	3word	Ethernet physical address (MAC-ID). If 11-22-33-44-55-66, then 0x2211, 0x4433, 0x6655.

* Power off and then power on, this value is applied.

3.3.4. Adapter Information Special Register (0x1100, 4352)

Address	Access	Type, Size	Description
0x1100(4352)			Reserved.
0x1101(4353)			Reserved.
0x1102(4354)	Read	1word	Start address of input image word register. =0x0000
0x1103(4355)	Read	1word	Start address of output image word register. =0x0800
0x1104(4356)	Read	1word	Size of input image word register.
0x1105(4357)	Read	1word	Size of output image word register.
0x1106(4358)	Read	1word	Start address of input image bit. = 0x0000
0x1107(4359)	Read	1word	Start address of output image bit. =0x1000
0x1108(4360)	Read	1word	Size of input image bit.
0x1109(4361)	Read	1word	Size of output image bit.
0x110D(4365)	Read/Write	1word	Enable/Disable Auto Reboot when FnBus, 0:Disable(Default)
0x110E(4366)	Read	upto 33word	Expansion slot's ST-number including NA. First 1word is adapter's number, if NA-9289, then 0x9289
0x1110(4368)	Read	1word	Number of expansion slot
0x1111(4369)	Read	1word	Number of active slot
0x1112(4370)	Read	1word	Number of inactive slot
0x1113(4371)	Read	upto 33word	Expansion slot Module Id. Refer to Appendix A.1 Product List. First 1word is adapter's module id.
0x1114(4372)*	Read/Write	1word	Input process image mode. The default value is 2. Valid value range is from 0 to 3. Refer to 2.4.2

0x1115(4373)*	Read/Write	1word	Output process image mode. The default value is 0. Valid value range is from 0 to 1. Refer to 2.4.3
0x1116(4374) **	Read/Write	2word	Inactive slot list, The corresponding bit represents slot position. 0:Active slot, 1:Inactive slot. Ex) if value is 0x0001, 0x8000, then slot#1,#32 are inactive slots
0x1117(4375)	Read	2word	Live slot list. , The corresponding bit represents slot position. 1:live slot, 0:not live slot
0x1118(4376)	Read	2word	Alarm slot list. The corresponding bit represents slot position. 1:Alarm slot, 0:Normal slot
0x1119(4377)	Read	1word	Hi byte is ModBus status, low byte is FnBus status. Refer to 2.4.2 It is identical with address 0x1040.
0x111A(4378)	Write	1word	Reserved. Adapter Scan command.
0x111B(4379)	Read/Write	1word	Reserved. IO State machine.
0x111C(4380)	Read	2word	Reserved. Runtime fault code.
0x111D(4381)	Read	1word	Adapter FnBus Revision. If 0x013C, FuBus Revision is 1.60
0x111E(4382)	Read	1word	Reserved. Adapter IO identification vendor code.
0x111F(4383)	Read	5word	LED Display Value and Status Code, TBD

* ** After the system is reset, the new "Set Value" action is applied.
** If the slot location is changed, set default value automatically (all expansion slot are live).

3.3.5. Expansion Slot Information Special Register (0x2000, 8192)

Each expansion slot has 0x20(32) address offset and same information structure.

Slot#1 0x2000(8192)~0x201F(8223) Slot#2 0x2020(8224)~0x203F(8255)
Slot#3 0x2040(8256)~0x205F(8287) Slot#4 0x2060(8288)~0x207F(8319)
Slot#5 0x2080(8320)~0x209F(8351) Slot#6 0x20A0(8352)~0x20BF(8383)
Slot#7 0x20C0(8384)~0x20DF(8415) Slot#8 0x20E0(8416)~0x20FF(8447)
Slot#9 0x2100(8448)~0x211F(8479) Slot#10 0x2120(8480)~0x213F(8511)
Slot#11 0x2140(8512)~0x215F(8543) Slot#12 0x2160(8544)~0x217F(8575)
Slot#13 0x2180(8576)~0x219F(8607) Slot#14 0x21A0(8608)~0x21BF(8639)
Slot#15 0x21C0(8640)~0x21DF(8671) Slot#16 0x21E0(8672)~0x21FF(8703)
Slot#17 0x2200(8704)~0x221F(8735) Slot#18 0x2220(8736)~0x223F(8767)
Slot#19 0x2240(8768)~0x225F(8799) Slot#20 0x2260(8800)~0x227F(8831)
Slot#21 0x2280(8832)~0x229F(8863) Slot#22 0x22A0(8864)~0x22BF(8895)
Slot#23 0x22C0(8896)~0x22DF(8927) Slot#24 0x22E0(8928)~0x22FF(8959)
Slot#25 0x2300(8960)~0x231F(8991) Slot#26 0x2320(8992)~0x233F(9023)
Slot#27 0x2340(9024)~0x235F(9055) Slot#28 0x2360(9056)~0x237F(9087)
Slot#29 0x2380(9088)~0x239F(9119) Slot#30 0x23A0(9120)~0x23BF(9151)
Slot#31 0x23C0(9152)~0x23DF(9183) Slot#32 0x23E0(9184)~0x23FF(9215)
Slot#32 0x2400(9216)~0x241F(9247) Slot#33 0x2420(10208)~0x243F(10239)
…..
Slot#61 0x2780(10112)~0x279F(10143) Slot#62 0x27A0(10144)~0x27BF(10175)
Slot#63 0x27C0(10176)~0x27DF(10207) Slot#64 0x27E0(10208)~0x27FF(10239)

Address Offset	Expansion Slot#1	Expansion Slot#2	Expansion Slot#3	…….	Expansion Slot#31	Expansion Slot#32
+ 0x00(+0)	0x2000(8192)	0x2020(8224)	0x2040(8256)	…….	0x23C0(9152)	0x23E0(9184)
+ 0x01(+1)	0x2001(8193)	0x2021(8225)	0x2041(8257)	…….	0x23C1(9153)	0x23E1(9185)
+ 0x02(+2)	0x2002(8194)	0x2022(8226)	0x2042(8258)	…….	0x23C2(9154)	0x23E2(9186)
+ 0x03(+3)	0x2003(8195)	0x2023(8227)	0x2043(8259)	…….	0x23C3(9155)	0x23E3(9187)
+ 0x04(+4)	0x2004(8196)	0x2024(8228)	0x2044(8260)	…….	0x23C4(9156)	0x23E4(9188)

+ 0x05(+5)	0x2005(8197)	0x2025(8229)	0x2045(8261)	…….	0x23C5(9157)	0x23E5(9189)
+ 0x06(+6)	0x2006(8198)	0x2026(8230)	0x2046(8262)	…….	0x23C6(9158)	0x23E6(9190)
+ 0x07(+7)	0x2007(8199)	0x2027(8231)	0x2047(8263)	…….	0x23C7(9159)	0x23E7(9191)
+ 0x08(+8)	0x2008(8200)	0x2028(8232)	0x2048(8264)	…….	0x23C8(9160)	0x23E8(9192)
+ 0x09(+9)	0x2009(8201)	0x2029(8233)	0x2049(8265)	…….	0x23C9(9161)	0x23E9(9193)
+ 0x0A(+10)	0x200A(8202)	0x202A(8234)	0x204A(8266)	…….	0x23CA(9162)	0x23EA(9194)
+ 0x0B(+11)	0x200B(8203)	0x202B(8235)	0x204B(8267)	…….	0x23CB(9163)	0x23EB(9195)
+ 0x0C(+12)	0x200C(8204)	0x202C(8236)	0x204C(8268)	…….	0x23CC(9164)	0x23EC(9196)
+ 0x0D(+13)	0x200D(8205)	0x202D(8237)	0x204D(8269)	…….	0x23CD(9165)	0x23ED(9197)
+ 0x0E(+14)	0x200E(8206)	0x202E(8238)	0x204E(8270)	…….	0x23CE(9166)	0x23EE(9198)
+ 0x0F(+15)	0x200F(8207)	0x202F(8239)	0x204F(8271)	…….	0x23CF(9167)	0x23EF(9199)
+ 0x10(+16)	0x2010(8208)	0x2030(8240)	0x2050(8272)	…….	0x23D0(9168)	0x23F0(9200)
+ 0x11(+17)	0x2011(8209)	0x2031(8241)	0x2051(8273)	…….	0x23D1(9169)	0x23F1(9201)
+ 0x12(+18)	0x2012(8210)	0x2032(8242)	0x2052(8274)	…….	0x23D2(9170)	0x23F2(9202)
+ 0x13(+19)	0x2013(8211)	0x2033(8243)	0x2053(8275)	…….	0x23D3(9171)	0x23F3(9203)
+ 0x14(+20)	0x2014(8212)	0x2034(8244)	0x2054(8276)	…….	0x23D4(9172)	0x23F4(9204)
+ 0x15(+21)	0x2015(8213)	0x2035(8245)	0x2055(8277)	…….	0x23D5(9173)	0x23F5(9205)
+ 0x16(+22)	0x2016(8214)	0x2036(8246)	0x2056(8278)	…….	0x23D6(9174)	0x23F6(9206)
+ 0x17(+23)	0x2017(8215)	0x2037(8247)	0x2057(8279)	…….	0x23D7(9175)	0x23F7(9207)
+ 0x18(+24)	0x2018(8216)	0x2038(8248)	0x2058(8280)	…….	0x23D8(9176)	0x23F8(9208)
+ 0x19(+25)	0x2018(8217)	0x2038(8249)	0x2058(8281)	…….	0x23D9(9177)	0x23F9(9209)
+ 0x1A(+26)	0x201A(8218)	0x203A(8250)	0x205A(8282)	…….	0x23DA(9178)	0x23FA(9210)
+ 0x1B(+27)	0x201B(8219)	0x203B(8251)	0x205B(8283)	…….	0x23DB(9179)	0x23FB(9211)
+ 0x1C(+28)	0x201C(8220)	0x203C(8252)	0x205C(8284)	…….	0x23DC(9180)	0x23FC(9212)
+ 0x1D(+29)	0x201D(8221)	0x203D(8253)	0x205D(8285)	…….	0x23DD(9181)	0x23FD(9213)
+ 0x1E(+30)	0x201E(8222)	0x203E(8254)	0x205E(8286)	…….	0x23DE(9182)	0x23FE(9214)
+ 0x1F(+31)	0x201F(8223)	0x203F(8255)	0x205F(8287)	…….	0x23DF(9183)	0x23FF(9215)

Address Offset	Access	Type, Size	Description
+ 0x00(+0)	Read	1word	Slot module id. Refer to Appendix A.1 Product List.
+ 0x01(+1)	Read	1word	Expansion Slot IO code. Refer to Table IO Data Code Format.
+ 0x02(+2) **	Read	1word	Input start register address of input image word this slot.
+ 0x03(+3) **	Read	1word	Input word's bit offset of input image word this slot.
+ 0x04(+4) **	Read	1word	Output start register address of output image word this slot.
+ 0x05(+5) **	Read	1word	Output word's bit offset of output image word this slot.
+ 0x06(+6) **	Read	1word	Input bit start address of input image bit this slot.
+ 0x07(+7) **	Read	1word	Output bit start address of output image bit this slot.
+ 0x08(+8) **	Read	1word	Size of input bit this slot
+ 0x09(+9) **	Read	1word	Size of output bit this slot
+ 0x0A(+10)**	Read	n word	Read input data this slot
+ 0x0B(+11)**	Read/Write	n word	Read/write output data this slot
+ 0x0C(+12) *	Read/Write	1word	Inactive slot, 0x0000:active, 0x0001:inactive
+ 0x0E(+14)	Read	1word	ST-number, if ST-1324, returns 0x1324
+ 0x0F(+15)	Read	String upto 74byte	First 1word is length of valid character string. If ST-1324, returns "00 21 53 54 2D 31 33 32 34 2C 20 46 6E 49 4F 20 34 20 53 6F 75 72 63 69 6E 67 20 49 6E 20 34 38 56 64 63 00" Valid character size = 0x0021 =33 characters, "ST-1324, FnIO 4 Sourcing In 48Vdc"
+ 0x10(+16)	Read	1word	Size of configuration parameter byte
+ 0x11(+17)**	Read/Write	n word	Read/write Configuration parameter data, up to 8byte. Refer to A.2 ***
+ 0x12(+18)	Read	1word	Size of memory byte.
+ 0x13(+19)**	Read/Write	n word	Read/write Memory data. Offset of memory is fixed with 0

+ 0x14(+20)**	Read/Write	n word	Read/write Memory data. First 2byte of write data is memory offset.
+ 0x15(+21)	Read	2word	Product code Refer to Appendix A.1 Product List.
+ 0x16(+22)	Read	2word	Catalog number. Refer to Appendix A.1 Product List.
+ 0x17(+23)	Read	1word	Firmware Revision
+ 0x18(+24)	Read	1word	FuBus Revision
+ 0x1A(+26)	Read/Write	n word	Reserved. Read/write expansion class access. (vendor only)
+ 0x1B(+27)	Read/Write	n word	Reserved. Read/write maintenance data access. (vendor only)

* After the system is reset, the new "Set Value" action is applied.
** Nothing of output, input, memory or configuration parameter corresponding slot returns Exception 02.
*** Slot Configuration parameter saved by internal EEPROM during power cycle until slot position changed.
*** All of output modules and special modules have the slot configuration parameter data. Refer to A.2.

- **Table 3.3.1. IO Data Code Format (1word)**

Item	**#15**	**#14**	**#13**	**#12**	**#11**	**#10**	**#9**	**#8**	**#7**	**#6**	**#5**	**#4**	**#3**	**#2**	**#1**	**#0**	**Word**
Field	Output IO code								Input IO code								
Field	Date Type		Data Length						Data Type		Data Length						
Example)																	
ST-3214	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0x0084
ST-1224	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0x00C4
ST-1228	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0x0041
ST-4123	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0x8200
ST-221F	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0x4200
ST-2324	1	1	0	0	0	1	0	0	1	1	0	0	0	1	0	0	0xC4C4

Input/Output Data Type :
0 0: No I/O Data
0 1: Byte Data
1 0: Word Data
1 1: Bit Data
Input/Output Data Length:
0 0 0 0 0 0 0 : 0 Bit/Byte/Word
0 0 0 0 0 0 1 : 1 Bit/Byte/Word
0 0 0 0 0 1 0 : 2 Bit/Byte/Word
0 0 0 0 0 1 1 : 3 Bit/Byte/Word

…

1 1 1 1 1 1 1 : 63 Bit/Byte/Word

3.4. MODBUS Reference

MODBUS Reference Documents
http://www.modubs.org
MODBUS Tools
http://www.modbustools.com, modbus poll
http://www.win-tech.com, modscan32

APPENDIX A

A.1. Product List

No.	ST-Number	Description	Module Id (hex)	Catalog Number (hex) +1,+0	Product Code (hex) +1,+0
	ST-1214	4-sinking input, 24Vdc	03	0003, 0041	83C0, 4001
	ST-1224	4-sourcing input, 24Vdc	04	0004, 0041	83C0, 4001
	ST-1218	8-sinking input, 24Vdc	07	0007, 0041	00C0, 4001
	ST-1228	8-sourcing input, 24Vdc	08	0008, 0041	00C0, 4001
	ST-121F	16-sinking input, 24Vdc	13	0013, 0141	01C0, 4001
	ST-122F	16-sourcing input, 24Vdc	14	0014, 0141	01C0, 4001
	ST-1314	4-sinking input, 48Vdc	05	0005, 0041	83C0, 4001
	ST-1324	4-sourcing input, 48Vdc	06	0006, 0041	83C0, 4001
	ST-1804	4-ac input, 110Vac	09	0009, 0041	83C0, 4001
	ST-1904	4-ac input, 220Vac	0A	000A, 0041	83C0, 4001
	ST-2314	4-sinking output, 24Vdc 0.5A	0E	000E, 0081	C083, 8001
	ST-2324	4-sourcing output, 24Vdc 0.5A	10	0010, 0081	C083, 8001
	ST-2318	8-sinking output, 24Vdc 0.5A	11	0011, 0081	C000, 8001
	ST-2328	8-sourcing output, 24Vdc 0.5A	12	0012, 0081	C000, 8001
	ST-221F	16-sinking output, 24Vdc 0.3A	15	0015, 0181	C001, 8001
	ST-222F	16-sourcing output, 24Vdc 0.3A	16	0016, 0181	C001, 8001
	ST-2414	4-sinking output, diag, 24Vdc 0.5A	37	3700, 00C1	8383, C001
	ST-2424	4-sourcing output, diag, 24Vdc 0.5A	38	3800, 00C1	8383, C001
	ST-2514	4-sinking output, diag, 24Vdc 2A	35	3500, 00C1	8383, C001
	ST-2524	4-sourcing output, diag, 24Vdc 2A	36	3600, 00C1	8383, C001
	ST-2742	2-relay output, 230Vac 2A	0B	000B, 0081	C081, 8001
	ST-2852	2-triac output, 120Vac 0.5A	0C	000C, 0081	C081, 8001
	ST-3114	4-current analog input, 0~20mA, 12bit	1C	001C, 4341	43C0, 6003
	ST-3134	4-current analog input, 0~20mA, 14bit	1E	001E, 4341	43C0, 6003
	ST-3214	4-current analog input, 4~20mA, 12bit	1D	001D, 4341	43C0, 6803
	ST-3234	4-current analog input, 4~20mA, 14bit	1F	001F, 4341	43C0, 6803
	ST-3424	4-voltage analog input, 0~10V, 12bit	20	0020, 4341	43C0, 6003
	ST-3444	4-voltage analog input, 0~10V, 14bit	22	0022, 4341	43C0, 6003
	ST-3524	4-voltage analog input, -10~10V, 12bit	21	0021, 4341	43C0, 6003
	ST-3544	4-voltage analog input, -10~10V, 14bit	23	0023, 4341	43C0, 6003
	ST-3624	4-voltage analog input, 0~5V, 12bit	24	0024, 4341	43C0, 6003
	ST-3644	4-voltage analog input, 0~5V, 14bit	25	0025, 4341	43C0, 6003
	ST-3702	2-RTD/Resistance input	28	0028, 4141	41C0, 6803
	ST-3802	2-Thermocouple/mV input	2A	002A, 4141	41C0, 6803
	ST-4112	2-current analog output, 0~20mA, 12bit	2C	002C, 4181	C041, A003
	ST-4212	2-current analog output, 4~20mA, 12bit	2D	002D, 4181	C041, A003
	ST-4422	2-voltage analog output, 0~10Vdc, 12bit	2E	002E, 4181	C041, A003
	ST-4522	2-voltage analog output, -10~10Vdc, 12bit	2F	002F, 4181	C041, A003
	ST-4622	2-voltage analog output, 0~5Vdc, 12bit	30	0030, 4181	C041, A003
	ST-5101	1 Channel, High Speed Counter, 5Vdc	34	3405, 01C1	0501, D003
	ST-5111	1 Channel, High Speed Counter, 24Vdc	39	3905, 01C1	0501, D003
	ST-5241*	2-Axes Motion Controller	41	4107, 07C1	0707, D001
	ST-5211	RS232 Communication, 1Channel, RTS/CTS Flow Control	42	4205, 05C1	0505, D001
	ST-5212	RS232 Communication, 2Channel	43	430B, 0BC1	0B0B, D001

	ST-5221	RS422 Communication, 1Channel	44	4405, 05C1	0505, D001
	ST-5231	RS485 Communication, 1Channel	45	4505, 05C1	0505, D001
	ST-5232	RS485 Communication, 2Channel	46	460B, 0BC1	0B0B, D001
	ST-2744	4-relay output, 230Vac 2A	51	0051, 0081	C083, 8001
	ST-2748	8-relay output, 230Vac 2A	50	0050, 0081	C000, 8001
	ST-1114	4-sinking input, 5Vdc	01	0001, 0041	83C0, 4001
	ST-1124	4-sourcing input, 5Vdc	02	0002, 0041	83C0, 4001
	ST-2114	4-TTL output inverting, 20mA	0D	000D, 0081	C083, 8001
	ST-2124	4-TTL output non-inverting, 20mA	0F	000F, 0081	C083, 8001
	ST-3428	8-voltage analog input, 0~10V, 12bit	80	0080, 4741	47C0, 6003
	ST-3118	8-current analog input, 0~20mA, 12bit	82	0082, 4741	47C0, 6003
	ST-3218	8-current analog input, 4~20mA, 12bit	83	0083, 4741	47C0, 6003
	ST-4424	4-voltage analog output, 0~10Vdc, 12bit	6A	006A, 4381	C043, A003
	ST-4114	4-current analog output, 0~20mA, 12bit	6D	006D, 4381	C043, A003
	ST-4214	4-current analog output, 4~20mA, 12bit	6E	006E, 4381	C043, A003
	ST-5422	2Ch PWM Output, 24Vdc 1.5A, Source	57	5701, 05C1	0105, E001
	ST-5442	2Ch PWM Output, 24Vdc 0.5A, Source	56	5601, 05C1	0105, E001
	ST-5444	4Ch PWM Output, 24Vdc 0.5A, Source	54	5401, 0BC1	030B, E001
	ST-5641	1Ch Pulse Output, 24Vdc 0.5A, Source	92	9203, 05C1	0305, E001
	ST-5642	2Ch Pulse Output, 24Vdc 0.5A, Source	90	9007, 09C1	0709, E001
	ST-5651	1Ch Pulse Output, 200KHz, RS422	98	9803, 05C1	0305, E001
	ST-5112	2Ch High Speed Counter Input, 100KHz, 24V	4D	4D07, 01C1	0701, E001
	ST-5114	4Ch High Speed Counter Input, 50KHz, 24V	4C	4C0F, 03C1	0F03, E001
	ST-5351	1Ch SSI Interface, 62.5K~2MHz, 30bit	9E	9E09, 01C1	0901, E001
	ST-111F	16-sinking input, 5Vdc	19	0019, 0141	01C0, 4001
	ST-112F	16-sourcing input, 5Vdc	1A	001A, 0141	01C0, 4001
	ST-131F	16-sinking input, 48Vdc	17	0017, 0141	01C0, 4001
	ST-132F	16-sourcing input, 48Vdc	18	0018, 0141	01C0, 4001
	ST-7111	Expansion System Power, 24V In, 1A/5V Out	Adpter can't recongnize it automatically		
	ST-7241	Field Power Isolator, AC/DC	"		
	ST-7008	Field Power Potential Dist, Shield(FG)	"		
	ST-7108	Field Power Potential Dist, DC 0V/AC L2	"		
	ST-7118	Field Power Potential Dist, DC 24V/AC L1	"		
	ST-7188	Field Power Potential Dist, DC 24V,0V/AC L1,L2	"		
	ST-7111A	Expansion System Power, 24V In, 1A/5V Out	E0	00E0, 0002	C0C0, 0001
	ST-7241A	Field Power Isolator, AC/DC	E2	00E2, 0002	C0C0, 0001
	ST-7008A	Field Power Potential Dist, Shield(FG)	E4	00E4, 0002	C0C0, 0001
	ST-7108A	Field Power Potential Dist, DC 0V/AC L2	E5	00E5, 0002	C0C0, 0001
	ST-7118A	Field Power Potential Dist, DC 24V/AC L1	E6	00E6, 0002	C0C0, 0001
	ST-7188A	Field Power Potential Dist, DC 24V,0V/AC L1,L2	E7	00E7, 0002	C0C0, 0001
	ST-3704	4-RTD/Resistance input, 20pin Connector	64	0064, 4341	43C0, 6003
	ST-3708	8-RTD/Resistance input, 20pin Connector	65	0065, 4741	47C0, 6003
	ST-3804	4-Thermocouple/mV input, 20pin Connector	66	0066, 4341	43C0, 6003
	ST-3808	8-Thermocouple/mV input, 20pin Connector	67	0067, 4741	47C0, 6003