

MODBUS TCP Network Adapter

NA-9289

User Manual



Version 1.01

2016 CREVIS Co.,Ltd

DOCUMENT CHANGE SUMMARY				
REV	PAGE	REMARKS	DATE	EDITOR
1.00	New Document		2014/10/17	YMKIM
1.01	15p, 16p, 24p	Modbus 232 port pin map, Module mounting and how to supply power correctly added	2016/12/05	YSKIM

CONTENTS

- 1. Important Notes 6
 - 1.1. Safety Instruction 7
 - 1.1.1. Symbols 7
 - 1.1.2. Safety Notes 7
- 2. Specification 8
 - 2.1. The Interface 8
 - 2.1.1. NA-9289(MODBUS TCP) 8
 - 2.2. Specification 9
 - 2.2.1. General Specification 9
 - 2.2.2. Interface Specification 10
 - 2.3. LED Indicator 11
 - 2.3.1. Module Status LED (MOD) 11
 - 2.3.2. Physical Connection LED (LINK) 11
 - 2.3.3. Exchange Data/Traffic Present LED(ACTIVE) 11
 - 2.3.4. Expansion Module Status LED (IOS) 12
 - 2.3.5. Field Power Status LED 12
- 3. Dimension 13
 - 3.1. NA-9289 13
- 4. Mechanical Setup 14
 - 4.1. Total Expansion 14
 - 4.2. Plugging and Removal of the Components 14
 - 4.3. Module mounting 15

4.4	How to supply the power correctly.....	16
5.	Convenience Function.....	17
5.1.	Web Server	17
5.2	IAP Functionality.....	18
6.	MODBUS Electrical Interface	20
6.1.	FnBus System.....	20
6.2.	FnBus Pin Description	22
6.3.	Communication Interface	23
6.3.1.	NA-9289.....	23
6.3.2.	DIP Switch	24
6.3.3.	RS232 port for MODBUS/RTU(for touch panel and IOGuidePro)	24
6.3.4.	MODBUS/TCP IP Address Setup.....	25
6.3.5.	I/O Process Image Map	29
6.3.6.	MODBUS Interface Register / Bit Map.....	29
6.4.	MODBUS/TCP Electrical Interface.....	30
6.4.1.	Example of Input Process Image(Input Register) Map	30
6.4.2.	Example of Output Process Image(Output Register) Map	33
7.	MODBUS/TCP INTERFACE	35
7.1.	MODBUS/TCP Protocol	35
7.1.1.	Comparison of MODBUS/TCP And MODBUS/RTU	35
7.1.2.	MODBUS/TCP MBAP Header	36
7.2.	Supported MODBUS Function Codes.....	36
7.2.1.	1 (0x01) Read Coils	37

7.2.2.	2 (0x02) Read Discrete Inputs	37
7.2.3.	3 (0x03) Read Holding Registers	38
7.2.4.	4 (0x04) Read Input Registers	39
7.2.5.	5 (0x05) Write Single Coil	40
7.2.6.	6 (0x06) Write Single Register	41
7.2.7.	8 (0x08) Diagnostics	42
7.2.8.	15 (0x0F) Write Multiple Coils.....	44
7.2.9.	16 (0x10) Write Multiple Registers	45
7.2.10.	23 (0x17) Read/Write Multiple Registers	46
7.2.11.	Error Response	47
7.3.	MODBUS Special Register Map.....	48
7.3.1.	Adapter Identification Special Register (0x1000, 4096).....	48
7.3.2.	Adapter Watchdog Time, other Time Special Register (0x1020, 4128)	49
7.3.3.	Adapter TCP/IP Special Register (0x1040, 4160)	50
7.3.4.	Adapter Information Special Register (0x1100, 4352).....	51
7.3.5.	Expansion Slot Information Special Register (0x2000, 8192).....	52
7.4.	MODBUS Reference.....	54
8.	Trouble Shooting.....	55
8.1.	How to diagnose by LED indicator.....	55

1. Important Notes

Solid state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls describes some important differences between solid state equipment and hard-wired electromechanical devices.

Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

In no event will CREVIS be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, CREVIS cannot assume responsibility or liability for actual use based on the examples and diagrams.

Warning!



- ✓ **If you don't follow the directions, it could cause a personal injury, damage to the equipment or explosion**
- Do not assemble the products and wire with power applied to the system. Else it may cause an electric arc, which can result into unexpected and potentially dangerous action by field devices. Arching is explosion risk in hazardous locations. Be sure that the area is non-hazardous or remove system power appropriately before assembling or wiring the modules.
- Do not touch any terminal blocks or IO modules when system is running. Else it may cause the unit to an electric shock or malfunction.
- Keep away from the strange metallic materials not related to the unit and wiring works should be controlled by the electric expert engineer. Else it may cause the unit to a fire, electric shock or malfunction.

Caution!


- ✓ **If you disobey the instructions, there may be possibility of personal injury, damage to equipment or explosion. Please follow below Instructions.**
- Check the rated voltage and terminal array before wiring. Avoid the circumstances over 55°C of temperature. Avoid placing it directly in the sunlight.
- Avoid the place under circumstances over 85% of humidity.
- Do not place Modules near by the inflammable material. Else it may cause a fire.
- Do not permit any vibration approaching it directly.
- Go through module specification carefully, ensure inputs, output connections are made with the specifications. Use standard cables for wiring.
- Use Product under pollution degree 2 environment.

1.1. Safety Instruction

1.1.1. Symbols

<p>DANGER</p> 	<p>Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death property damage or economic loss.</p>
<p>IMPORTANT</p>	<p>Identifies information that is critical for successful application and understanding of the product.</p>
<p>ATTENTION</p> 	<p>Identifies information about practices or circumstances that can lead to personal injury, property damage, or economic loss. Attentions help you to identify a hazard, avoid a hazard, and recognize the consequences.</p>

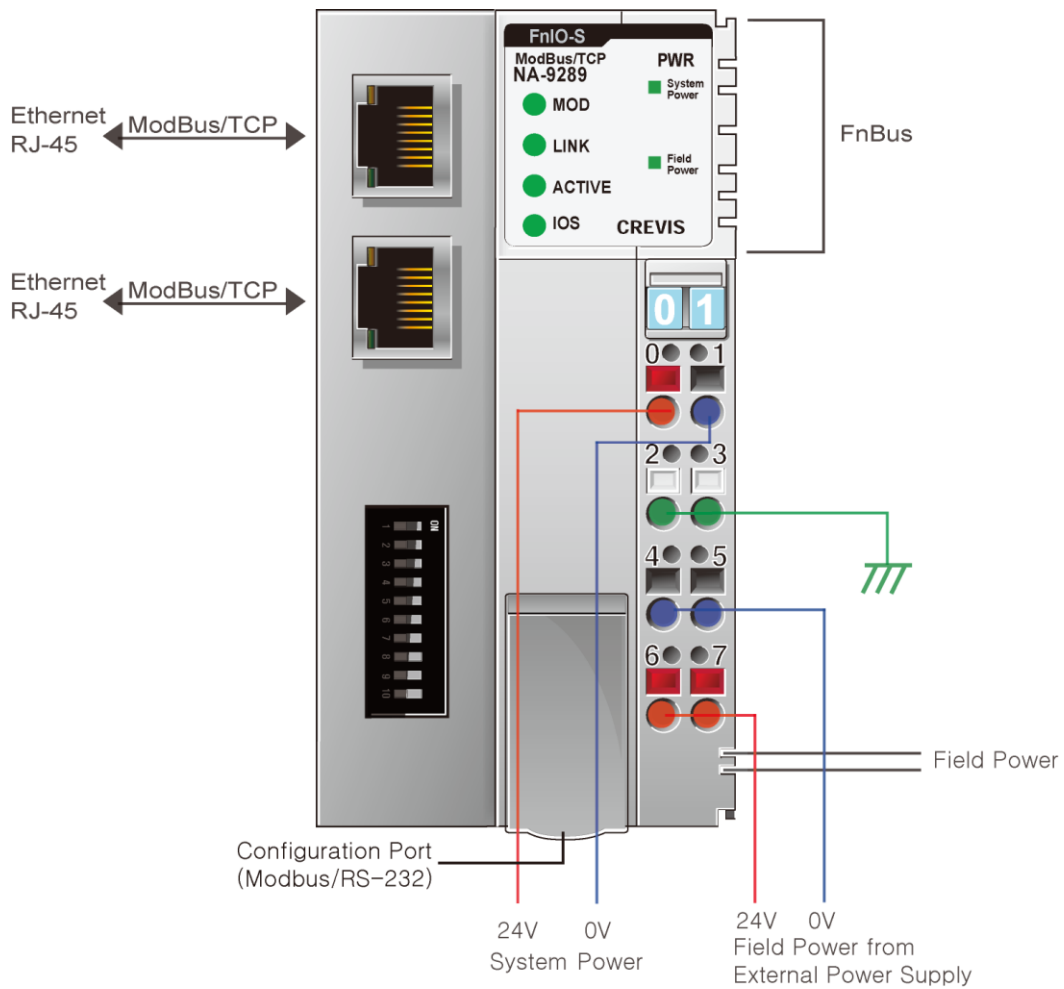
1.1.2. Safety Notes

<p>DANGER</p> 	<p>The modules are equipped with electronic components that may be destroyed by electrostatic discharge. When handling the modules, ensure that the environment (persons, workplace and packing) is well grounded. Avoid touching conductive components, e.g. FnBUS Pin.</p>
--	--

2. Specification

2.1. The Interface

2.1.1. NA-9289(MODBUS TCP)



⚠ Caution!

System power and Field power must be supplied separately.

2.2. Specification

2.2.1. General Specification

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 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	
Environmental Specifications	
Operating Temperature	-20 °C ~55 °C
Storage Temperature	-40 °C ~85 °C
Relative Humidity	5% ~ 90% non-condensing
Mounting	DIN rail
General Specifications	
Shock Operating	IEC 60068-2-27
Vibration/shock resistance	Sine Vibration (Based on IEC 60068-2-6) 5 ~ 25Hz : ±1.6mm 25 ~ 300Hz : 4g Sweep Rate : 1 Oct/min, 20 Sweeps Random Vibration (Based on IEC 60068-2-64) 10 ~ 40Hz : 0.0125g ² /Hz 40 ~ 100Hz : 0.0125 → 0.002g ² /Hz 100 ~ 500Hz : 0.002g ² /Hz 500 ~ 2000Hz : 0.002 → 1.3 x 10 ⁻⁴ g ² /Hz Test time : 1hrs for each test
EMC resistance burst/ESD	EN 61000-6-2 : 2005, EN 61000-6-4/A11 : 2011
Installation Pos. / Protect. Class	Variable/IP20
Product Certifications	UL, cUL, CE, FCC, KCC, RoHS(EU,China)

2.2.2. Interface Specification

Interface Specification, NA-9289 (MODBUS/TCP Server)	
Adapter Type	Slave node (MODBUS/TCP, MODBUS/UDP Server)
Max. Expansion Module	63 slots
Max. Input Size	126words (252bytes)
Max. Output Size	126words (252bytes)
Max. Length Bus Line	Up to 100m 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, BOOTP, HTTP
Interface Connector	RJ-45 socket * 2pcs
IP Address Setup	Via BOOTP/DHCP or IOGuide(Crevis Configuration Software)
IP-Address range	xxx.xxx.xxx.1 ~ 253 (User area) xxx.xxx.xxx.254 ~ 255 (Reserved for IAP Function)
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

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	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	Flashing Green	Adapter (Slave) exchange data/Traffic present. About 10msec flashing.

2.3.4. Expansion 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
FnBus connection fault during exchanging IO	Red	One or more expansion module occurred in fault state. - Changed expansion module configuration. - FnBus communication failure.
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.

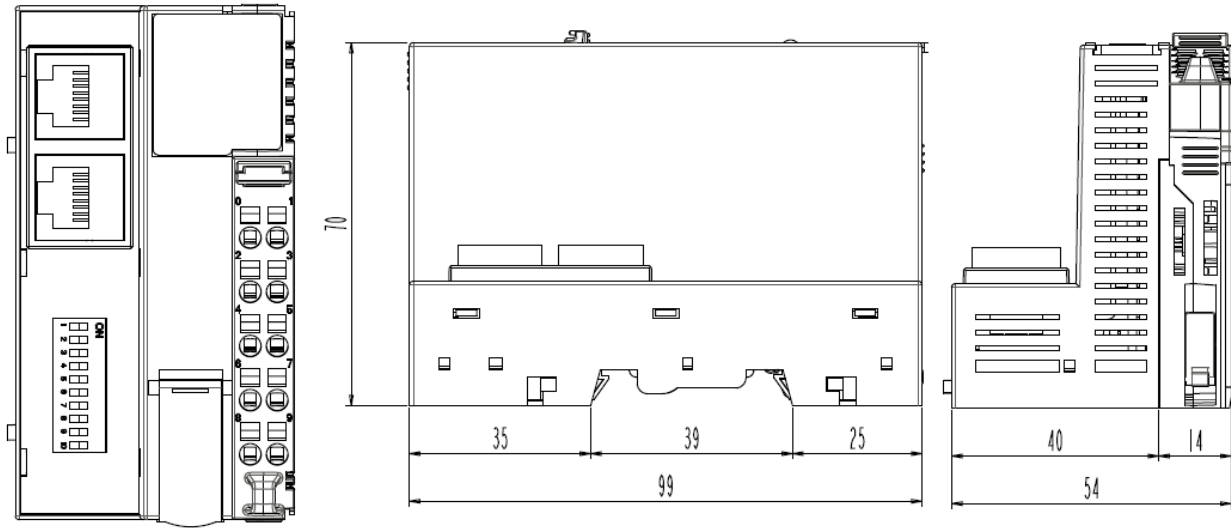
2.3.5. Field Power Status LED

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

3. Dimension

3.1. NA-9289

(mm)

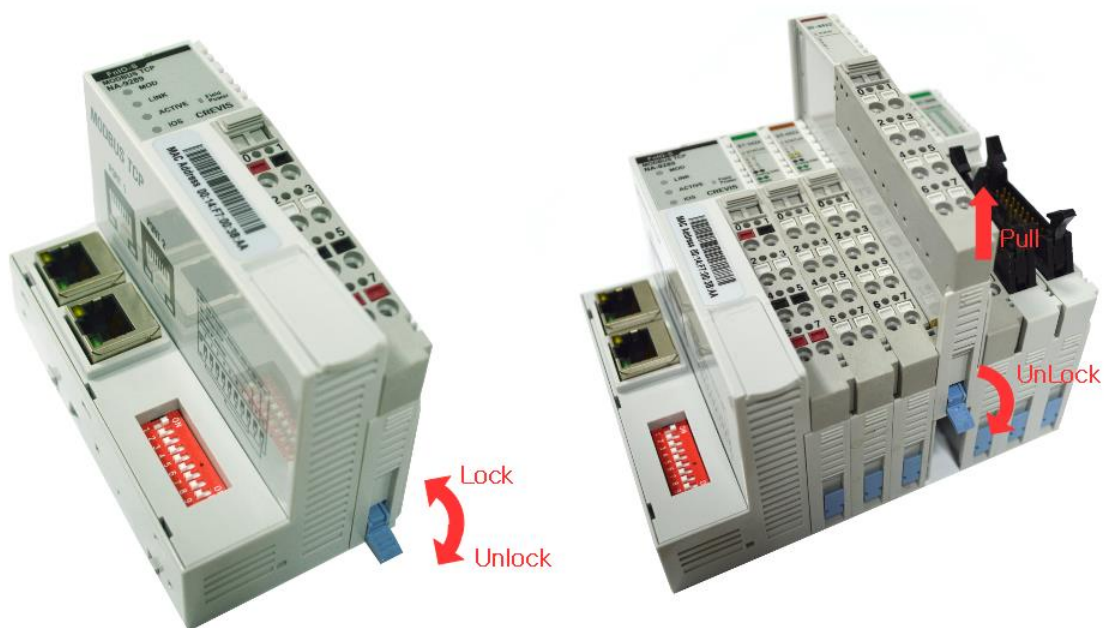


4. Mechanical Setup

4.1. Total Expansion


The number of the module assembly that can be connected is 63. So the maximum length is 426mm Exception. ST-2748 is excepted to calculate maximum length because that is double width module.

4.2. Plugging and Removal of the Components.



As above figure in order to safeguard the FnIO module from jamming, it should be fixed onto the DIN rail with locking level. To do so, fold on the upper of the locking lever.

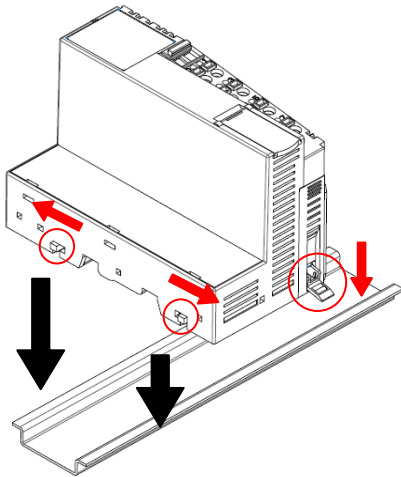
To pull out the FnIO module, unfold the locking lever as below figure.

<p>DANGER</p> 	<p>Before work is done on the components, the voltage supply must be turned off.</p>
--	--

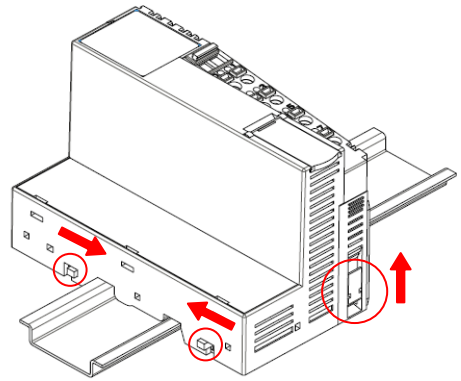
4.3 Module mounting

How to mount on DIN-rail

- ① Press down the module lightly on the DIN-rail
- ※ DIN-rail lockers and lever should be unlocked in this step.

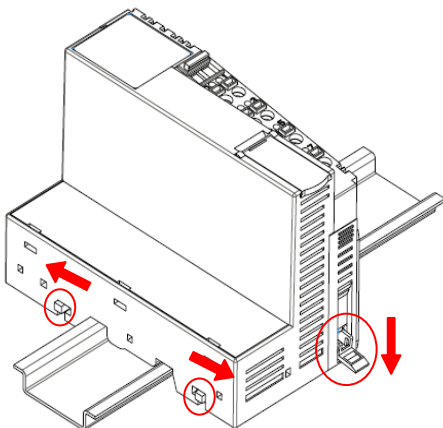


- ② Lock DIN-rail lockers and lever in right direction

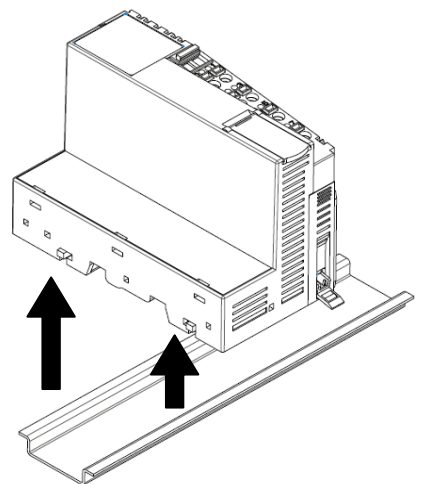


How to dismount from DIN-rail

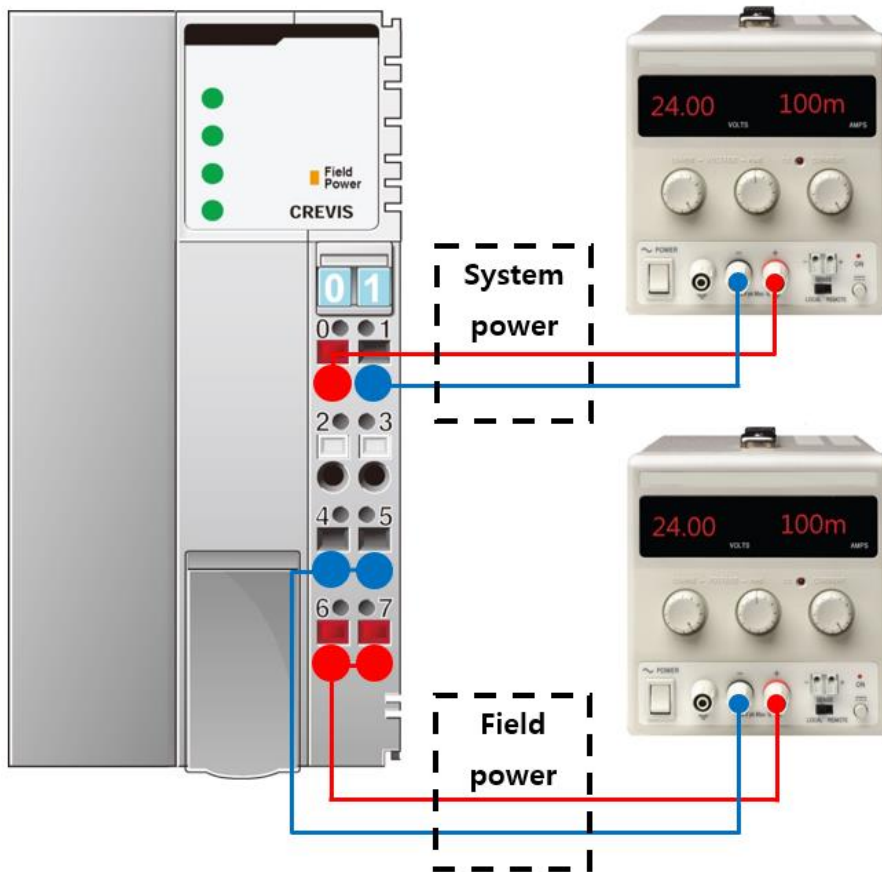
- ① Unlock DIN-rail lockers and lever in right direction



- ② Pull up the module to remove from the DIN-rail



4.4 How to supply the power correctly



- Refer the pin map of power RTB before wiring.
- Current capacity margin should be considered when you supply the power.
- Supply voltage 24Vdc which is recommended voltage level.
- **System and Field power must be supplied separately as the picture above.**

※ If the power is supplied to each System and Field power from same power source, it would be vulnerable to power noise.

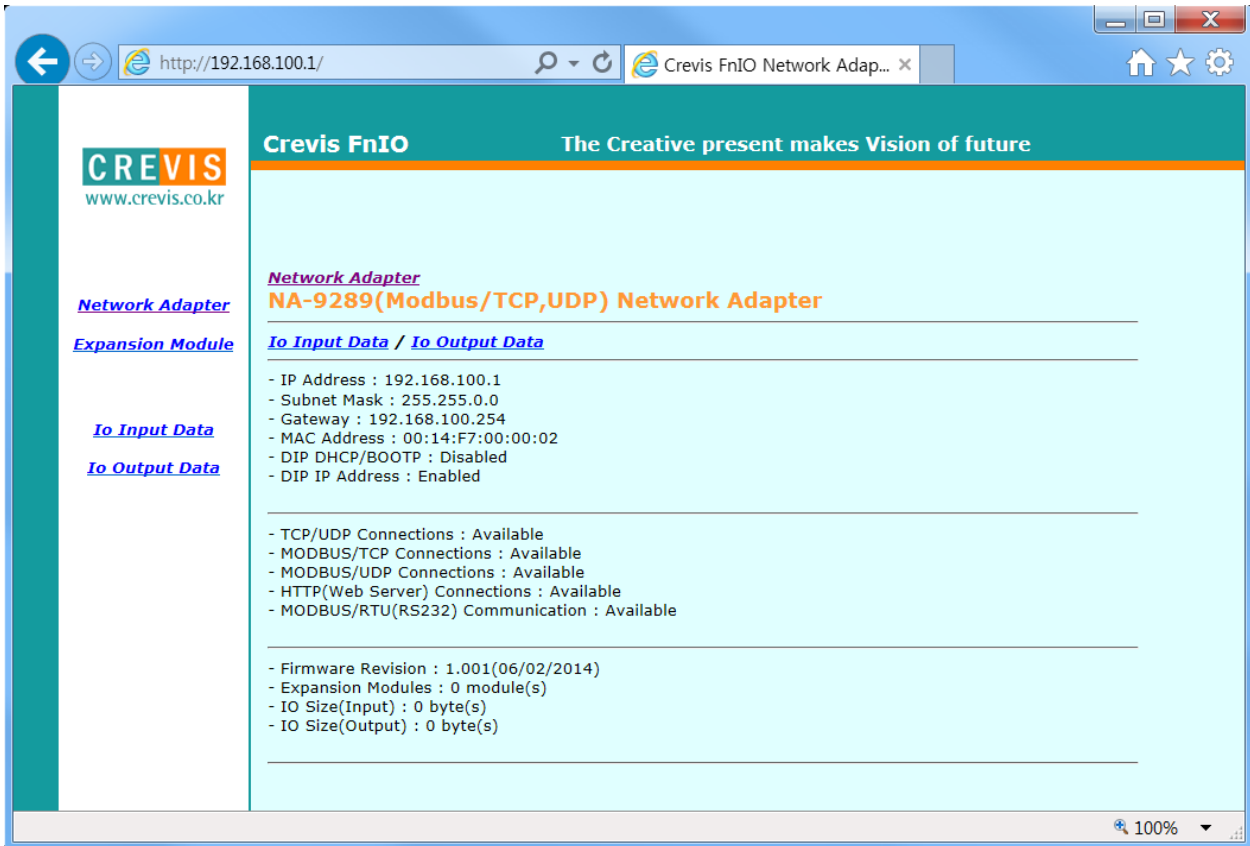
5. Convenience Function

5.1. Web Server

NA-9289's IP addresses can be set as "XXX.XXX.XXX. 1 to 253".

After setting up its IP address, enter its IP address to the web.

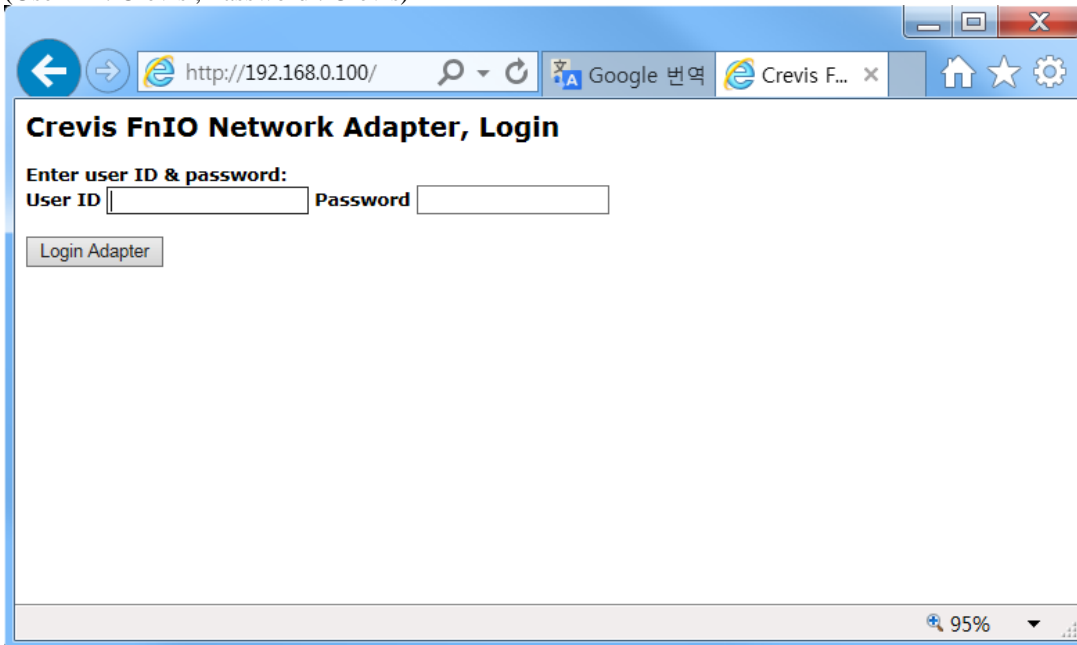
Then, NA-9289's basic information such as its status, configuration and etc. will be checked via its web browser.



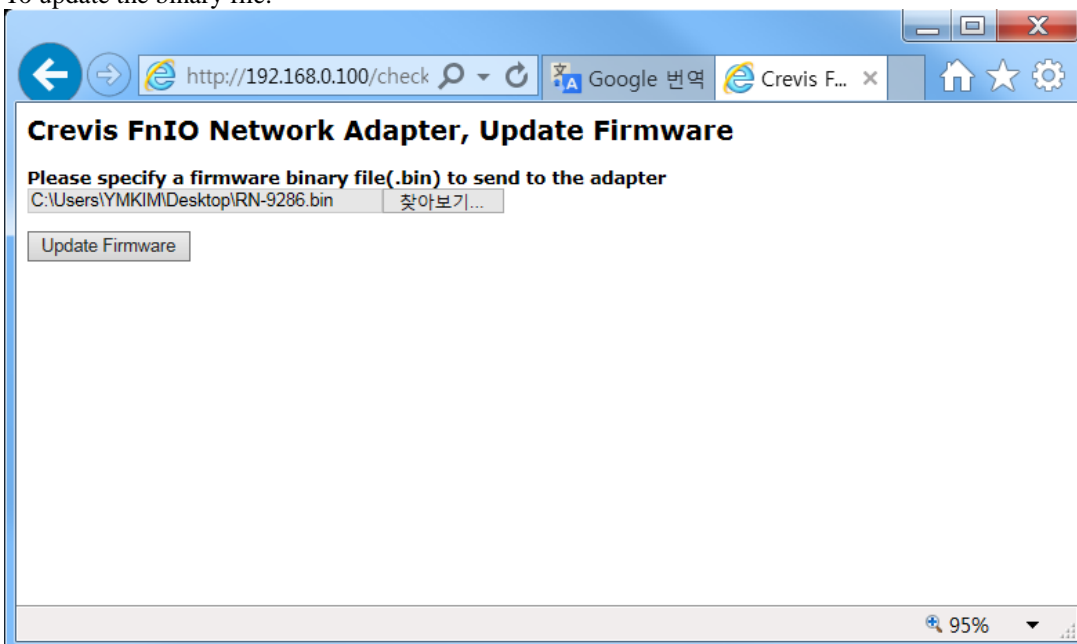
5.2 IAP Functionality.

After setting up the dip switch as 254 or 255, Power off and on in order to start the IAP mode.
(254= Fixed IP Address(192.168.0.100) / 255= Last used IP Address)

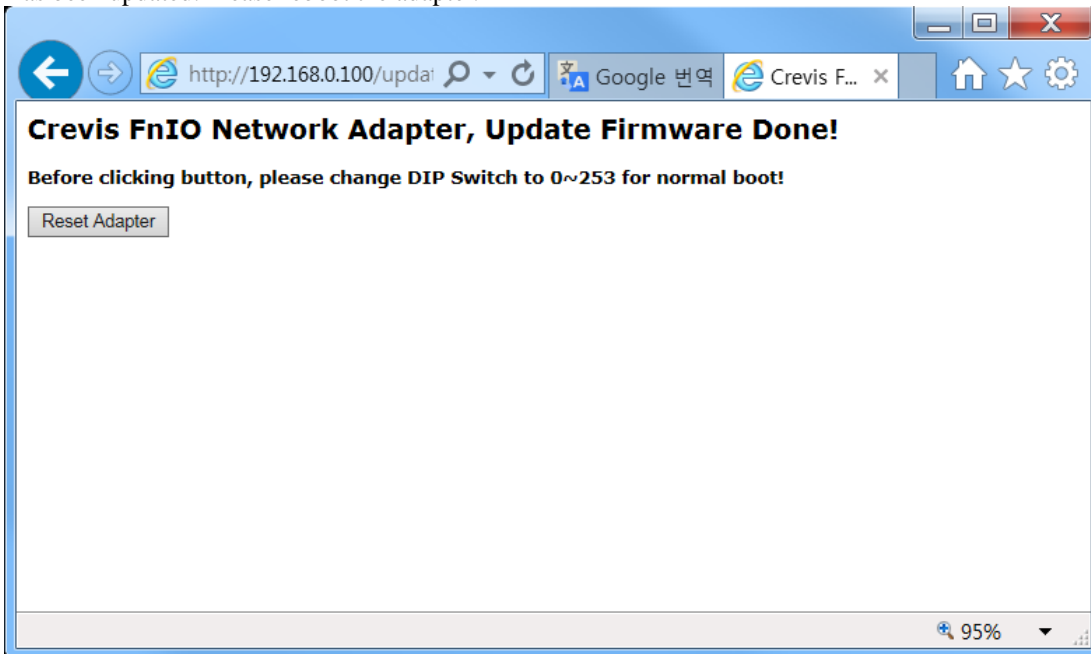
After Login the Web Browser connecting.
(User ID : Crevis , Password : Crevis)



To update the binary file.

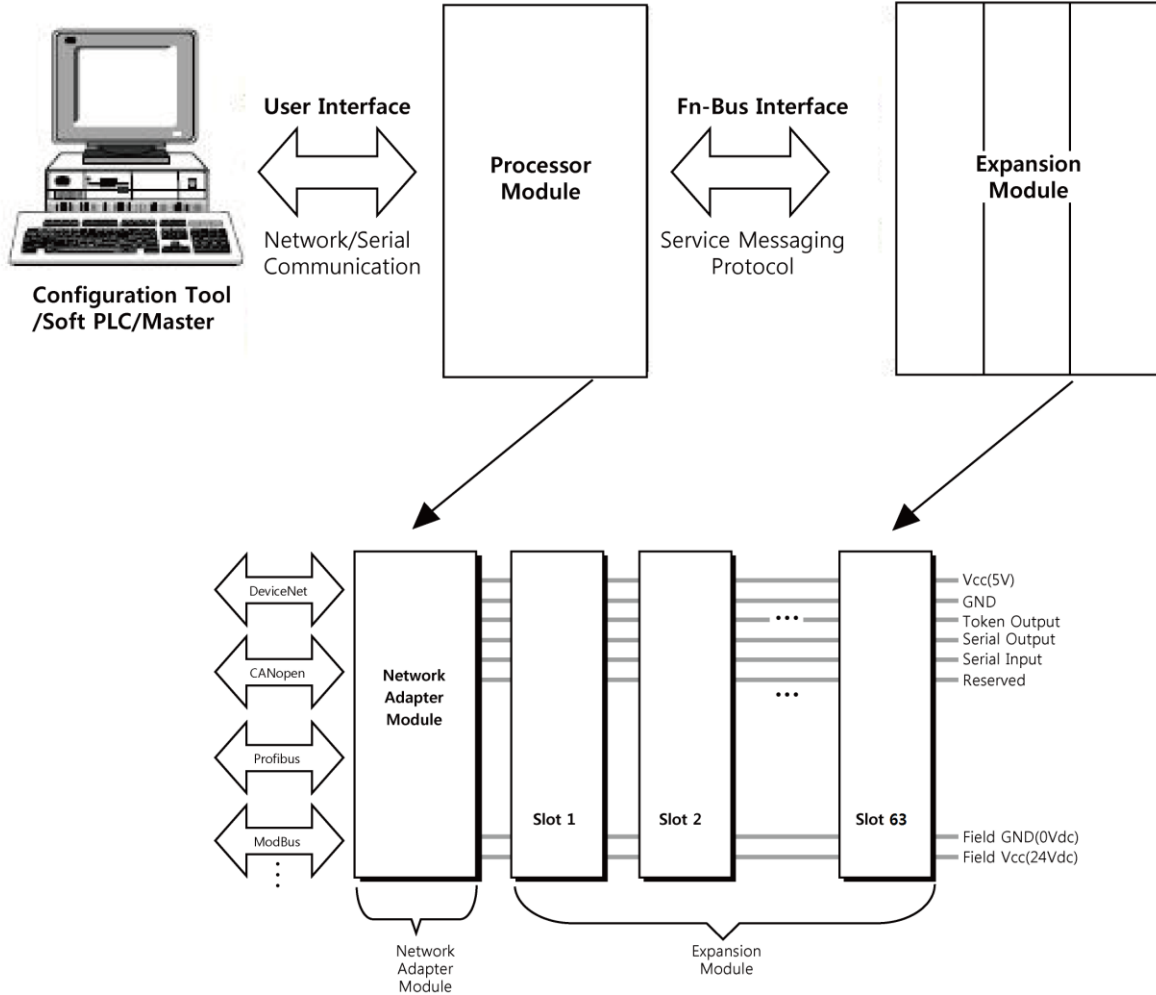


Has been updated. Please reboot the adapter.



6. MODBUS Electrical Interface

6.1. FnBus System



- **Network Adapter Module**

The Network Adapter Module forms the link between the field bus and the field devices with the Expansion Modules.

The connection to different field bus systems can be established by each of the corresponding Network Adapter Module, e.g. for SyncNet, PROFIBUS, CANopen, DeviceNet, Ethernet/IP, CC-Link, MODBUS/Serial, MODBUS/TCP etc.

- **Expansion Module**

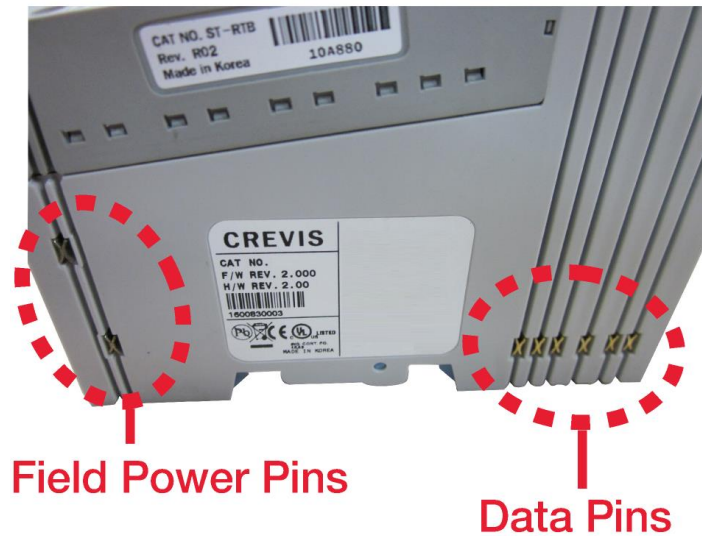
The Expansion Modules are supported a variety of input and output field devices. There are digital and analog input/output modules and special function modules.

- **Two types of FnBus Message**

- Service Messaging
- I/O Messaging

6.2. FnBus Pin Description

Communication between the NA series and the expansion module as well as system / field power supply of the bus modules is carried out via the internal bus. It is comprised of 6 data pin and 2 field power pin.



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).

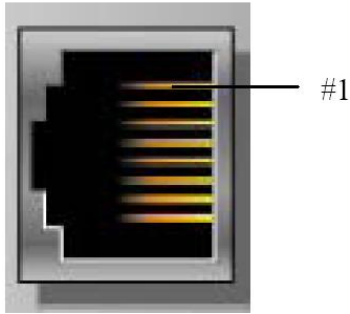
DANGER



Do not touch data and field power pins in order to avoid soiling and damage by ESD noise.

6.3. Communication Interface

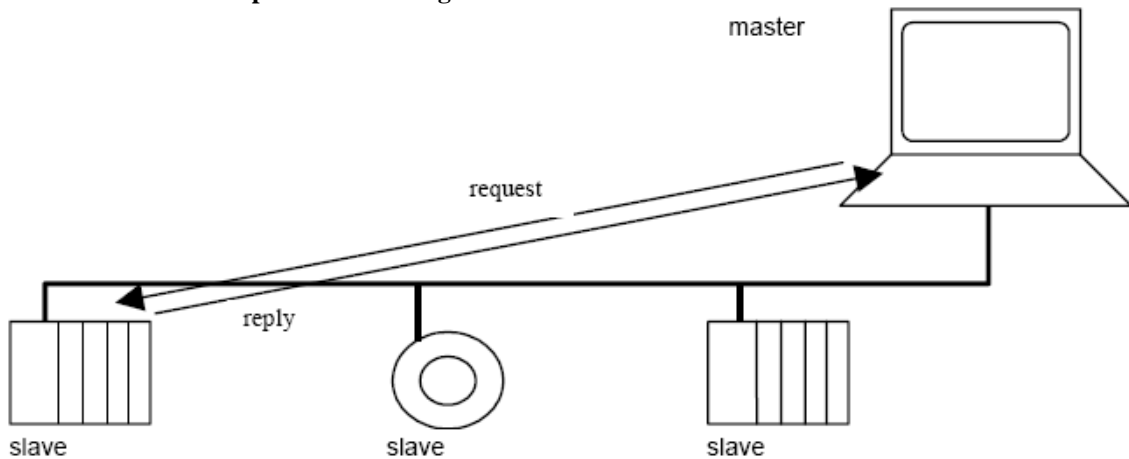
6.3.1. NA-9289



Shielded RJ-45 Socket

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

MODBUS/TCP Network Setup is like following.

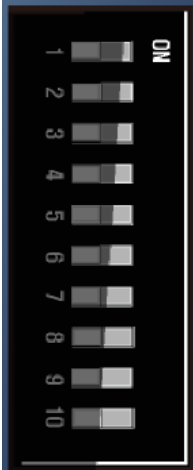


ATTENTION



The use of an incorrect supply voltage or frequency can cause severe damage to the component.

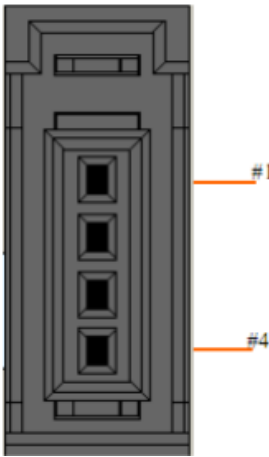
6.3.2. DIP Switch



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/BOOTP *	
10	=ON : Use Lowest IP Address with IP_DIP value	

*DHCP/BOOTP have to be set in special register(default : BOOTP). (0x1045).

6.3.3. RS232 port for MODBUS/RTU(for touch panel and IOGuidePro)



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

6.3.4. MODBUS/TCP IP Address Setup

- **IP-Address Setup using by DIP switch (Manual function)**

If the adapter DIP Pole#10 is ON, lowest IP address is set by DIP Pole#1~#8 manually.
These are examples of adapter IP-Address setup by manual function.

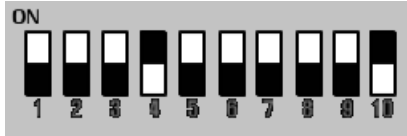
Ex) xxx . xxx . xxx . 1



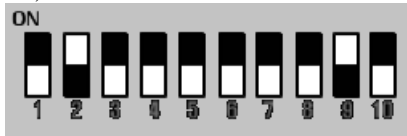
Ex) xxx . xxx . xxx . 2



Ex) xxx . xxx . xxx . 8



Ex) xxx . xxx . xxx . 253



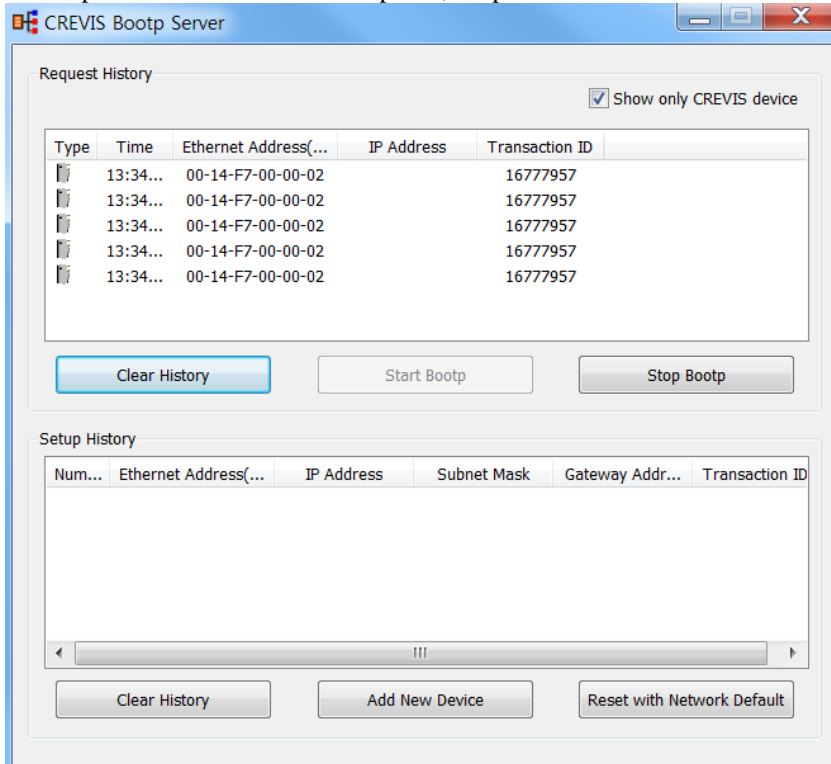
- **IP-Address Setup using BOOTP/DHCP Server**

The following is an example of adapter IP-Address setup using CREVIS IO Guide Pro's BOOTP server.

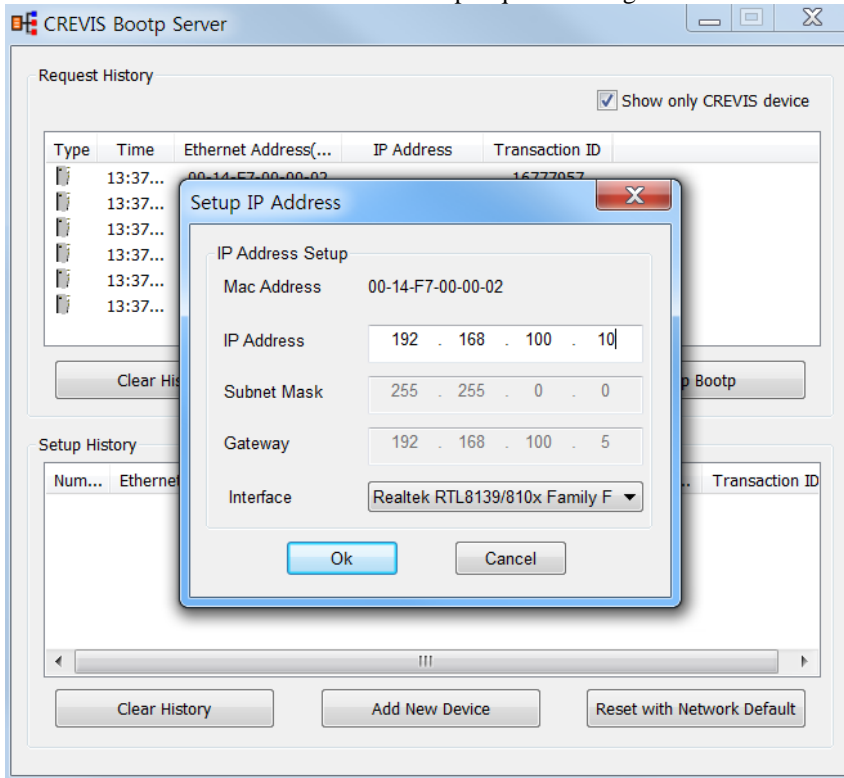
Click 'Start Bootp' to enable Bootp server to detect Bootp request on the network.

If the adapter is Bootp/DHCP enabled (Dip Pole #9 ON), adapter will send Bootp/DHCP request 20times every 5seconds, after power reset.

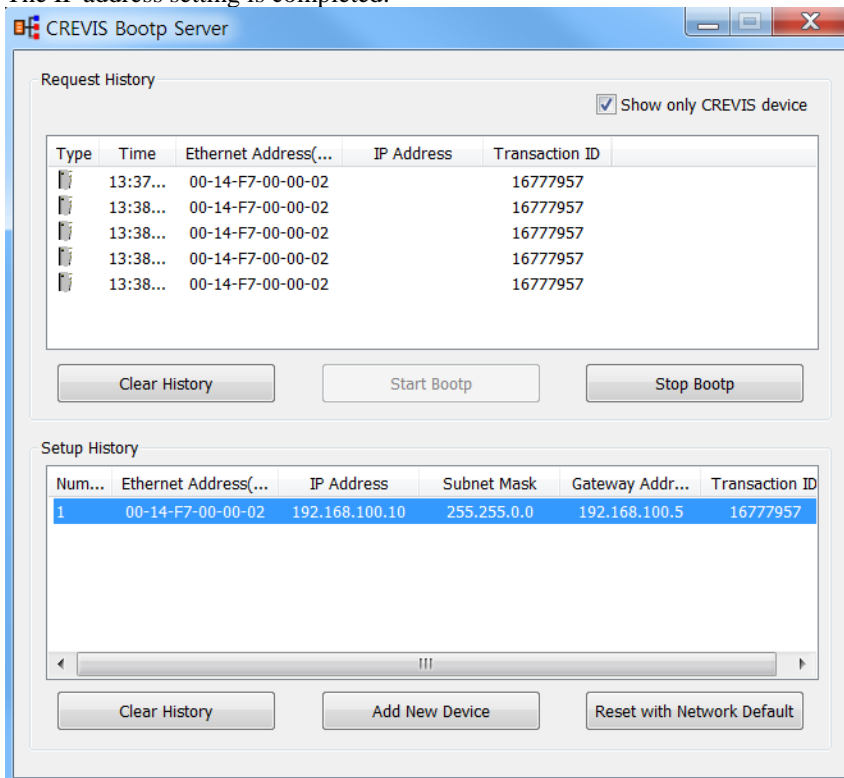
If Bootp/DHCP server does not response, adapter will use the latest saved IO address in EEPROM.



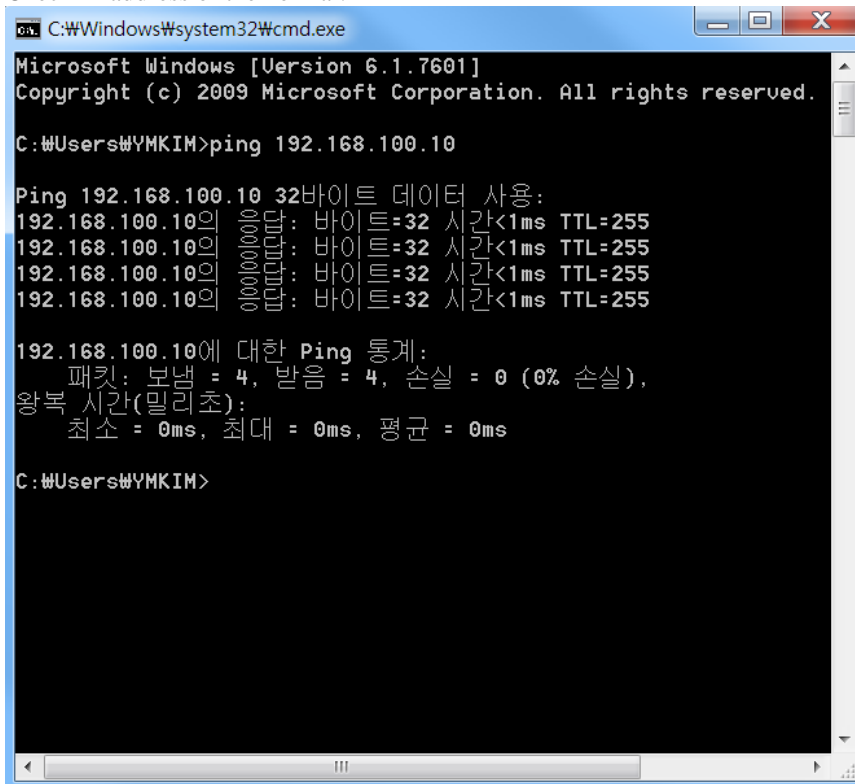
Double-click on one of the detected 'Boot request message' and set the IP address.



The IP address setting is completed.



Check IP address of the normal.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\#YMKIM>ping 192.168.100.10

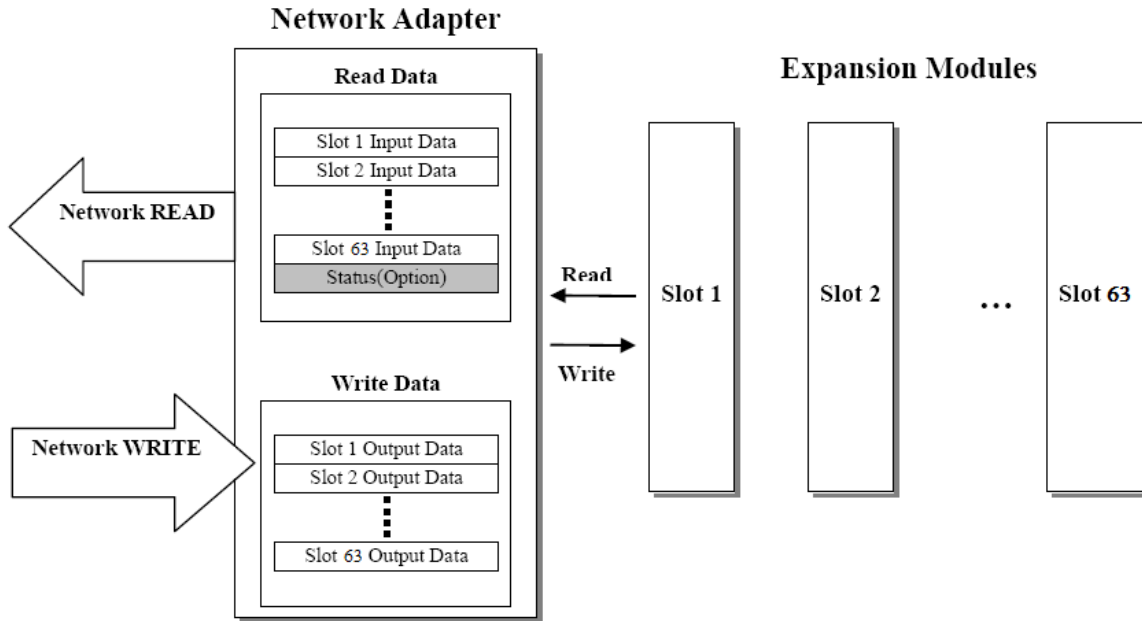
Ping 192.168.100.10 32바이트 데이터 사용:
192.168.100.10의 응답: 바이트=32 시간<1ms TTL=255
192.168.100.10의 응답: 바이트=32 시간<1ms TTL=255
192.168.100.10의 응답: 바이트=32 시간<1ms TTL=255
192.168.100.10의 응답: 바이트=32 시간<1ms TTL=255

192.168.100.10에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
    왕복 시간(밀리초):
        최소 = 0ms, 최대 = 0ms, 평균 = 0ms

C:\Users\#YMKIM>
```

6.3.5. 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.



6.3.6. 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

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

● **Bit Map**

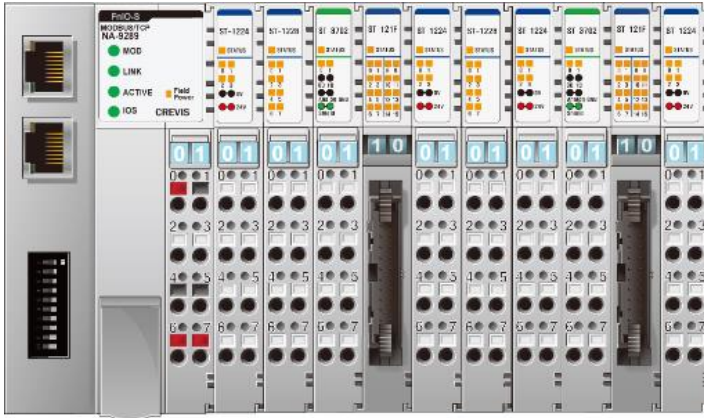
Start Address	Read/Write	Description	Func. Code
0x0000 ~	Read	Process input image bits All input registers area is addressable by bit address. Size of input image bit is size of input image register * 16.	2
0x1000 ~	Read/Write	Process output image bits All output registers area is addressable by bit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

6.4. MODBUS/TCP Electrical Interface

6.4.1. 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 6.3.3.

● 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

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

Status (1 word)

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.

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

Status (1word)	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)							Empty, 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.

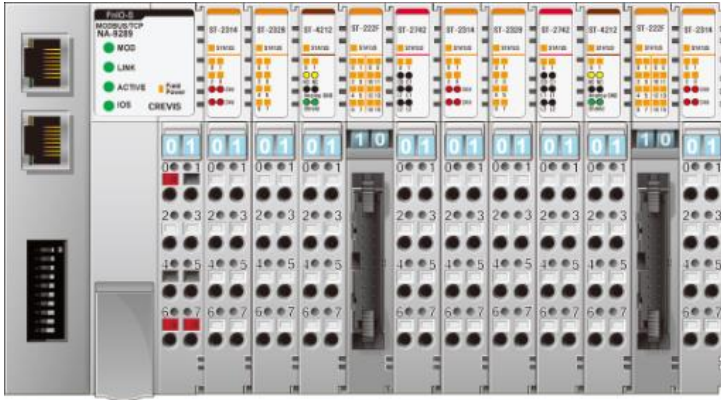
✓ **Input Assembly Priority :**

- 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)

6.4.2. 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 6.3.3.

● 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-relay output
#8	2-relay 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 out Ch0 high byte (Slot#3)								Analog out Ch0 low byte (Slot#3)							
0x0802	Analog out Ch1 high byte (Slot#3)								Analog out 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 out Ch0 high byte (Slot#9)								Analog out Ch0 low byte (Slot#9)							
0x0807	Analog out Ch1 high byte (Slot#9)								Analog out Ch1 low byte (Slot#9)							
0x0808	Discrete out high 8pts (Slot#10)								Discrete out 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 out Ch0 high byte (Slot#3)								Analog out Ch0 low byte (Slot#3)							
0x0801	Analog out Ch1 high byte (Slot#3)								Analog out Ch1 low byte (Slot#3)							
0x0802	Analog out Ch0 high byte (Slot#9)								Analog out Ch0 low byte (Slot#9)							
0x0803	Analog out Ch1 high byte (Slot#9)								Analog out Ch1 low byte (Slot#9)							
0x0804	Discrete out low 8pts (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 input image bit is size of input 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)

7. MODBUS/TCP INTERFACE

7.1. MODBUS/TCP Protocol

The MODBUS messaging service provides a Client/Server communication between devices connected on an Ethernet TCP/IP network. All MODBUS/TCP messages are sent via TCP on registered port 502.

7.1.1. Comparison of MODBUS/TCP And MODBUS/RTU

This header provides some differences compared to the MODBUS RTU application data unit used on serial line:

- ✓ The MODBUS ‘slave addresses’ 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 chars	1 char	1 char	Up to 252 chars	2 chars	≥ 3.5 chars

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

7.1.2. MODBUS/TCP MBAP Header

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

Fields	Length	Description	Client	Server
Transaction Identifier	2 bytes	Identification of a MODBUS Request /Response transaction.	Initialized by the client	Recopied by the server from the received
Protocol Identifier	2 bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received
Length	2 bytes	Number of following bytes	Initialized by the client (Request)	Initialized by the server (Response)
Unit Identifier	1 byte	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.*

7.2. 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 (Serial Line only)	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 register	Read a number of input words / Write a number of output words

- Refer to MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1a

7.2.1. 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 Output Hi	0x00
Quantity of Output Lo	0x0A

● Response

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

- In case of address 0x1015~0x1000 output bit value: 00000010_01010101.

7.2.2. 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 output bit value: 00000000_10000000.

7.2.3. 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.

7.2.4. 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.

7.2.5. 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
Starting Address Hi	0x10
Starting Address Lo	0x01
Quantity of Outputs Hi	0xFF
Quantity of Outputs 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.

7.2.6. 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
Starting Address Hi	0x08
Starting Address Lo	0x00
Quantity of Outputs Hi	0x11
Quantity of Outputs Lo	0x22

● Response

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

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

7.2.7. 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 makes the remote device to restart with factory default setup of EEPROM.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x0001(1)	0x0000, 0xFF00	Echo Request Data	Reset
0x0001(1)	0x55AA	Echo Request Data	Reset with Default Setting 1)
0x0001(1)	0x55AA+0xAB7B+Sumcheck 4)	Echo Request Data	Reset with Factory default 2)
0x0001(1)	0x55AA+0xAA55+Sumcheck 4)	Echo Request Data	Reset with Factory default 3)

- 1),2),3) All expansion slot configuration parameters are cleared.
- 2),3) IP Address, Subnet Mask Address, Gateway Address will be the factory defaults value.
- 3) Mac Address will be the factory default value.
- 4) Refer to 2.9.1 for Sumcheck (0x1006)

✓ **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 6.2.11.

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 1 word of input process image. Refer to 5.3.1.

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

✓ **Sub-function 0x0065(101) Return Slave MODBUS, 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

7.2.8. 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.

7.2.9. 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	0x00
Quantity of Outputs Hi	0x00
Quantity of Outputs Lo	0x02

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

7.2.10. 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
Write Reg. Value #0 Hi	0x11
Write Reg. Value #0 Lo	0x22
Write Reg. Value #1 Hi	0x33
Write Reg. Value #1 Lo	0x44

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

7.2.11. 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.

7.3. 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).

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

Address	Access	Type, Size	Description
0x1000(4096)	Read	1 word	Vendor ID = 0x02E5 (741), Crevis. Co., Ltd.
0x1001(4097)	Read	1 word	Device type = 0x000C, Network Adapter
0x1002(4098)	Read	1 word	Product Code = 0x8040
0x1003(4099)	Read	1 word	Firmware revision, if 0x0101, revision 1.01
0x1004(4100)	Read	2 words	Product unique serial number
0x1005(4101)	Read	String upto 34bytes	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	1 word	Sum check of EEPROM
0x1010(4112)	Read	2 words	Firmware release date
0x1011(4113)	Read	2 words	Product manufacturing inspection date
0x1012(4114)	Read	String upto 34bytes	Vendor name string First 1word is length of valid character string.
0x101E(4126)	Read	15 words	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.

7.3.2. 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	1 word	Watchdog time value 16bit unsigned. The time value is represented by multiples of 100msec. The default value is 0 (watchdog timeout disabled). A changing of watchdog time value resets watchdog error.
0x1021(4129)	Read	1 word	Watchdog time remain value This value decreases every 100msec
0x1022(4130)	Read	1 word	Watchdog error counter, it is cleared by writing address 0x1020
0x1023(4131)	Read/Write	1 word	Enable/disable auto recovery Watchdog error when receiving new frame. 0: Disable, 1: Enable (default). Its value is stored in EEPROM.
0x1028(4136)	Read	2 words	IO update time, main loop time. (100usec unit)

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

Address	Access	Type, Size	Description
0x1040(4160)	Read	1 word	MODBUS/TCP statistics. Same as input process image's status (1 word). Hi byte is MODBUS status, low byte is FnBus status. Refer to 5.3.1.
0x1041(4161)	Read/Write	1 word	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	1 word	Reserved. number of MODBUS/TCP connected
0x1043(4163)	Read	1 word	MODBUS/TCP port, fixed 502
0x1044(4164)	Read	1 word	Ethernet Interface Speed, 10(10Mbps) or 100(100Mbps)
0x1045(4165)	Read/Write	1 word	IP Setting Method, 0:BOOTP, 1:DHCP (Default : 0)
0x1046(4166)	---	---	
0x1047(4167)	Read	1 word	Status of DIP SW#9 DHCP/BOOTP(Enable/Disable). 0 : OFF, 1 : ON
0x1048(4168)	Read	1 word	Enable/disable Lowest IP address via DIP Switch, 1:Enabled
0x1050(4176)	Read/Write	2 words	IP address. If 192.168.100.32, then 0xA8C0, 0x2064. After update this value, IP address, Subnet mask and Gateway are applied as new one.
0x1051(4177)	Read/Write	2 words	Subnet mask. If 255.255.255.0, then 0xFFFF, 0x00FF.
0x1052(4178)	Read/Write	2 words	Gateway. If 192.168.123.254, then 0xA8C0, 0xFE7B.
0x1053(4179)	Read	3 words	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.

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

Address	Access	Type, Size	Description
0x1100(4352)			Reserved
0x1101(4353)			Reserved
0x1102(4354)	Read	1 word	Start address of input image word register. =0x0000
0x1103(4355)	Read	1 word	Start address of output image word register. =0x0800
0x1104(4356)	Read	1 word	Size of input image word register.
0x1105(4357)	Read	1 word	Size of output image word register.
0x1106(4358)	Read	1 word	Start address of input image bit. = 0x0000
0x1107(4359)	Read	1 word	Start address of output image bit. =0x1000
0x1108(4360)	Read	1 word	Size of input image bit.
0x1109(4361)	Read	1 word	Size of output image bit.
0x110D(4365)	Read	1 word	Field Power & Current Dip Switch State
0x110E(4366)	Read	Upto 33 words	Expansion slot's ST-number including NA. First 1word is adapter's number, if NA-9289, then 0x9289
0x1110(4368)	Read	1 word	Number of expansion slot
0x1111(4369)	Read	1 word	Number of active slot
0x1112(4370)	Read	1 word	Number of inactive slot
0x1113(4371)	Read	upto 33 words	Expansion slot Module Id. Refer to Appendix A.1 Product List. First 1word is adapter's module id.
0x1114(4372)*	Read/Write	1 word	Input process image mode. The default value is 2. Valid value range is from 0 to 3.
0x1115(4373)*	Read/Write	1 word	Output process image mode. The default value is 0. Valid value range is from 0 to 1.
0x1116(4374)**	Read/Write	2 words	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	2 words	Live slot list. , The corresponding bit represents slot position. 1: live slot, 0: not live slot
0x1118(4376)	Read	2 words	Alarm slot list. The corresponding bit represents slot position. 1:Alarm slot, 0:Normal slot
0x1119(4377)	Read	1 word	Hi byte is MODBUS status, low byte is FnBus status. It is identical with address 0x1040.
0x111A(4378)	Write	1 word	Reserved. Adapter Scan command.
0x111B(4379)	Read/Write	1 word	Reserved. IO State machine.
0x111C(4380)	Read	2 words	Reserved. Runtime fault code.
0x111D(4381)	Read	1 word	Adapter FnBus Revision. If 0x013C, FnBus Revision is 1.60
0x111E(4382)	Read	1 word	Reserved. Adapter IO identification vendor code.
0x111F(4383)	Read	5 words	LED Display Value and Status Code

*, ** After the system is reset, the new "Set Value" action is applied.

** If the slot location is changed, set default value automatically (all expansion slots are live).

7.3.5. 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#17	0x2200(8704) ~0x221F (8735)
Slot#2	0x2020(8224) ~0x203F (8255)	Slot#18	0x2220(8736) ~0x223F (8767)
Slot#3	0x2040(8256) ~0x205F (8287)	Slot#19	0x2240(8768) ~0x225F (8799)
Slot#4	0x2060(8288) ~0x207F (8319)	Slot#20	0x2260(8800) ~0x227F (8831)
Slot#5	0x2080(8320) ~0x209F (8351)	Slot#21	0x2280(8832) ~0x229F (8863)
Slot#6	0x20A0 (8352) ~0x20BF (8383)	Slot#22	0x22A0 (8864) ~0x22BF (8895)
Slot#7	0x20C0 (8384) ~0x20DF (8415)	Slot#23	0x22C0 (8896) ~0x22DF (8927)
Slot#8	0x20E0 (8416) ~0x20FF (8447)	Slot#24	0x22E0 (8928) ~0x22FF (8959)
Slot#9	0x2100(8448) ~0x211F (8479)	Slot#25	0x2300(8960) ~0x231F (8991)
Slot#10	0x2120(8480) ~0x213F (8511)	Slot#26	0x2320(8992) ~0x233F (9023)
Slot#11	0x2140(8512) ~0x215F (8543)	Slot#27	0x2340(9024) ~0x235F (9055)
Slot#12	0x2160(8544) ~0x217F (8575)	Slot#29	0x2360(9056) ~0x237F (9087)
Slot#13	0x2180(8576) ~0x219F (8607)
Slot#14	0x21A0 (8608) ~0x21BF (8639)	Slot#61	0x2780(10112)~0x279F(10143)
Slot#15	0x21C0 (8640) ~0x21DF (8671)	Slot#62	0x27A0(10144)~0x27BF(10175)
Slot#16	0x21E0 (8672) ~0x21FF (8703)	Slot#63	0x27C0(10176)~0x27DF(10207)

Address Offset	Expansion Slot#1	Expansion Slot#2	Expansion Slot#3	Expansion Slot#62	Expansion Slot#63
+ 0x00(+0)	0x2000(8192)	0x2020(8224)	0x2040(8256)	0x27C0(10176)	0x27E0(10208)
+ 0x01(+1)	0x2001(8193)	0x2021(8225)	0x2041(8257)	0x27C1(10177)	0x27E1(10209)
+ 0x02(+2)	0x2002(8194)	0x2022(8226)	0x2042(8258)	0x27C2(10178)	0x27E2(10210)
+ 0x03(+3)	0x2003(8195)	0x2023(8227)	0x2043(8259)	0x27C3(10179)	0x27E3(10211)
+ 0x04(+4)	0x2004(8196)	0x2024(8228)	0x2044(8260)	0x27C4(10180)	0x27E4(10212)
+ 0x05(+5)	0x2005(8197)	0x2025(8229)	0x2045(8261)	0x27C5(10181)	0x27E5(10213)
+ 0x06(+6)	0x2006(8198)	0x2026(8230)	0x2046(8262)	0x27C6(10182)	0x27E6(10214)
+ 0x07(+7)	0x2007(8199)	0x2027(8231)	0x2047(8263)	0x27C7(10183)	0x27E7(10215)
+ 0x08(+8)	0x2008(8200)	0x2028(8232)	0x2048(8264)	0x27C8(10184)	0x27E8(10216)
+ 0x09(+9)	0x2009(8201)	0x2029(8233)	0x2049(8265)	0x27C9(10185)	0x27E9(10217)
+ 0x0A(+10)	0x200A(8202)	0x202A(8234)	0x204A(8266)	0x27CA(10186)	0x27EA(10218)
+ 0x0B(+11)	0x200B(8203)	0x202B(8235)	0x204B(8267)	0x27CB(10187)	0x27EB(10219)
+ 0x0C(+12)	0x200C(8204)	0x202C(8236)	0x204C(8268)	0x27CC(10188)	0x27EC(10220)
+ 0x0D(+13)	0x200D(8205)	0x202D(8237)	0x204D(8269)	0x27CD(10189)	0x27ED(10221)
+ 0x0E(+14)	0x200E(8206)	0x202E(8238)	0x204E(8270)	0x27CE(10190)	0x27EE(10222)
+ 0x0F(+15)	0x200F(8207)	0x202F(8239)	0x204F(8271)	0x27CF(10191)	0x27EF(10223)
+ 0x10(+16)	0x2010(8208)	0x2030(8240)	0x2050(8272)	0x27D0(10192)	0x27F0(10224)
+ 0x11(+17)	0x2011(8209)	0x2031(8241)	0x2051(8273)	0x27D1(10193)	0x27F1(10225)
+ 0x12(+18)	0x2012(8210)	0x2032(8242)	0x2052(8274)	0x27D2(10194)	0x27F2(10226)
+ 0x13(+19)	0x2013(8211)	0x2033(8243)	0x2053(8275)	0x27D3(10195)	0x27F3(10227)
+ 0x14(+20)	0x2014(8212)	0x2034(8244)	0x2054(8276)	0x27D4(10196)	0x27F4(10228)
+ 0x15(+21)	0x2015(8213)	0x2035(8245)	0x2055(8277)	0x27D5(10197)	0x27F5(10229)
+ 0x16(+22)	0x2016(8214)	0x2036(8246)	0x2056(8278)	0x27D6(10198)	0x27F6(10230)
+ 0x17(+23)	0x2017(8215)	0x2037(8247)	0x2057(8279)	0x27D7(10199)	0x27F7(10231)
+ 0x18(+24)	0x2018(8216)	0x2038(8248)	0x2058(8280)	0x27D8(10200)	0x27F8(10232)
+ 0x19(+25)	0x2019(8217)	0x2039(8249)	0x2059(8281)	0x27D9(10201)	0x27F9(10233)
+ 0x1A(+26)	0x201A(8218)	0x203A(8250)	0x205A(8282)	0x27DA(10202)	0x27FA(10234)
+ 0x1B(+27)	0x201B(8219)	0x203B(8251)	0x205B(8283)	0x27DB(10203)	0x27FB(10235)
+ 0x1C(+28)	0x201C(8220)	0x203C(8252)	0x205C(8284)	0x27DC(10204)	0x27FC(10236)

+ 0x1D(+29)	0x201D(8221)	0x203D(8253)	0x205D(8285)	0x27DD(10205)	0x27FD(10237)
+ 0x1E(+30)	0x201E(8222)	0x203E(8254)	0x205E(8286)	0x27DE(10206)	0x27FE(10238)
+ 0x1F(+31)	0x201F(8223)	0x203F(8255)	0x205F(8287)	0x27DF(10207)	0x27FF(10239)

Address	Access	Type, Size	Description
+ 0x00(+0)	Read	1 word	Slot module id.
+ 0x01(+1)	Read	1 word	Expansion Slot IO code. Refer to Table IO Data Code Format.
+ 0x02(+2)**	Read	1 word	Input start register address of input image word this slot.
+ 0x03(+3)**	Read	1 word	Input word's bit offset of input image word this slot.
+ 0x04(+4)**	Read	1 word	Output start register address of output image word this slot.
+ 0x05(+5)**	Read	1 word	Output word's bit offset of output image word this slot.
+ 0x06(+6)**	Read	1 word	Input bit start address of input image bit this slot.
+ 0x07(+7)**	Read	1 word	Output bit start address of output image bit this slot.
+ 0x08(+8)**	Read	1 word	Size of input bit this slot
+ 0x09(+9)**	Read	1 word	Size of output bit this slot
+ 0x0A(+10)**	Read	n words	Read input data this slot
+ 0x0B(+11)**	Read/Write	n words	Read/write output data this slot
+ 0x0C(+12)*	Read/Write	1 word	Inactive slot, 0x0000:active, 0x0001:inactive
+ 0x0E(+14)	Read	1 word	ST-number, if ST-1324, returns 0x1324
+ 0x0F(+15)	Read	String upto 74 bytes	First 1 word 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	1 word	Size of configuration parameter byte
+ 0x11(+17)**	Read/Write	n words	Read/write Configuration parameter data, up to 8byte.
+ 0x12(+18)	Read	1 word	Size of memory byte.
+ 0x13(+19)**	Read/Write	n words	Read/write Memory data. Offset of memory is fixed with 0.
+ 0x14(+20)**	Read/Write	n words	Read/write Memory data. First 2byte of write data is memory offset.
+ 0x15(+21)	Read	2 words	Product code.
+ 0x16(+22)	Read	2 words	Catalog number.
+ 0x17(+23)	Read	1 word	Firmware Revision
+ 0x18(+24)	Read	1 word	FnBus Revision
+ 0x1A(+26)	Read/Write	n words	Reserved. Read/write expansion class access. (vendor only)
+ 0x1B(+27)	Read/Write	n words	Reserved. Read/write maintenance data access. (vendor only)

* After the system is reset, the new "Set Value" action is applied.

** Nothing of output, input, and 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 Document.
(FnIO_Configuration_Parameter_Memory_Register)

● IO Data Code Format (1 word)

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				Date 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 Bit/Byte/Word

0 0 0 0 0 1: 1 Bit/Byte/Word

0 0 0 0 1 0: 2 Bit/Byte/Word

0 0 0 0 1 1: 3 Bit/Byte/Word

.....

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

7.4. MODBUS Reference

MODBUS Reference Documents

<http://www.modbus.org>

MODBUS Tools

<http://www.modbustools.com> , MODBUS poll

<http://www.win-tech.com> , MODSCAN32

8. Trouble Shooting

8.1. How to diagnose by LED indicator

LED Status	Cause	Action
All LED turns off	- No power	- Check main power Cable
	- System power is not supplied.	- Contact Sales team and send module for repair.
MOD LED flashes green	- Failure of initialization EEPROM parameter.	- Contact Sales team and send module for repair.
MOD LED flashes red	- Excess of expansion slot - Excess of IO size - Wrong IO composition - Occurrence of EEPROM checksum error	- Use expansion slot up to 32. - Compose that IO total size is not excess. - Check composition I/O Module
MOD LED is red	- Wrong address ID - Occurrence critical error in firmware	- Contact Sales team and send module for repair.
I/O LED turns off	- Failure of realization expansion Module - None expansion Module	- Check connector status both NA series and expansion module.
I/O LED flashes red	Failure of configuration baud rate	- Check communication cable with Master - Check power for master.
	Failure of initialization I/O	- Use expansion slot up to 32. - Compose that IO total size is not excess. NA series notice unidentified expansion module ID. Check status of expansion module.
I/O LED is red	Failure of exchanging I/O data	Check status of expansion IO connection.
NET LED turns off	Failure of communication with Master	Check main power for master and communication cable.
NET LED flashed green	Failure of exchanging data with master	Check status in software for Master configuration.
NET LED is red	Communication connecting lost	Check BUS line cable for connection with master.
		Check duplication address.

8.2. How to diagnose when device couldn't communicate network

Inspection of wrong or omission cable connection.

- Check status of cable connection for each node.
- Check that all color matches between connector and cable.
- Check wire omission.

Terminator resistor

- If terminator resistor is not installed, install terminator resistor
- Check location of terminator resistor

Configuration of Node address

- Check duplication node address.

Configuration of Master

- Check configuration of master
- Check whether to do download or don't
- Check composition is right
- Configuration of communication baud rate
- I/O size
- Configuration of each node

Ground and environment

- Check ground is contacted
- Check environment factor (temperature, humidity, etc) is in less than regular limit