FnIO G-Series:

GL-9971

G-Series Light Version Programmable I/O

[History]

Rev.	Pages	Remarks	Date	Editor
1.00	-	Draft	2019.11.22	SH KIM
1.10	5, 9	All Specification	2019.12.16	SH KIM
1.20	5, 23	RTC Specfication, Modbus Register	2020.01.14	SH KIM
1.30	5	Add UL Specification	2020.03.12	SH KIM
1.40	5,7	RTC Specfication, diagram image	2021.01.05	MK PARK

Table of Contents

1. ENVIRONMENT SPECIFICATION

Environmental specification	
Operating Temperature	-20°C~60°C
UL Temperature	-20℃~60℃
Storage Temperature	-40℃~85℃
Relative Humidity	5% ~ 90% non-condensing
Mounting	DIN rail
Vibration Resistance	
EMC Resistance Burst/ESD	IEC 60068-2-27
Installation Pos. / Protect. Class	Based on IEC 60068-2-6 Sine Vibration 5 ~ 25Hz : 1.6mm 25 ~ 300Hz : 4g Sweep Rate : 1 Oct/min, 20 cycles Random Vibration 10 ~ 40Hz : 0.0125g²/Hz 40 ~ 100Hz : 0.0125 → 0.002g²/Hz 100 ~ 500Hz : 0.002g²/Hz 500 ~ 2000Hz : 0.002 → 1.3 x 10^{-4}g²/Hz Test time : 1hours for each test
Product Certifications	EN 61000-6-2 : 2005 EN 61000-6-4/A11 : 2011
Installation Position	Vertical and horizontal installation is vailable
Product Certifications	CE, UL, KC(TBD)

2. GL-9971 (G-SERIES LIGHT VERSION PROGRAMMABLE I/O)

2.1. Specification

Programmable Specification		
Programming	CoDeSys V3.5.11.3	
Program Memory	256 KBytes	
Data Memory	40 KBytes	IO Input: %IW0 ~%IW2047 (2048 words) IO Output: %QW0 ~%QW2047 (2048 words) Memory: %MW0 ~ %MW8191 (8192 words)
Non-Volatile Memory	4 KBytes (Retain : 2 KBytes, Flag : 2 KBytes)	
Run-Time System	Multiple PLC Tasks	
Program Languages	IEC 61131-3 (LD, IL, ST, FBD, SFC)	
RTC*	Retain Time : < 15 day / Accuracy : < 2min/month (Status : fully recharged battery at room temperature)	
Max. Task	10	
Max. Cycle Task	10	
Max. Status Task	10	
Process Time	1usec (90 Instructions)	

* RTC

Battery charging time	Retain time (room temperature)
4 hours	< 2 day
12 hours	< 12 day
16 hours	< 15 day

- Recommend charging for at least 16 hours when the battery is discharged.

* RTC Warning : There are 3 operating problems when the battery is discharged.
- Retain data will not be saved.
- RTC data will not be stored and is the initial value.
- Reset button will not work.(PLC Reset and Factory Reset cannot be used)

Interface Specification	
Adapter Type	Modbus TCP master/ slave node
Interface	RJ-45 socket * 2pcs
Baud rate	10/100Mbps, Auto-negotiation, Full Duplex
Ethernet Protocol	Modbus/TCP, Modbus/UDP, SNTP, HTTP (Web-Server), DHCP/BOOTP
Max. Socket	16 (UDP: 10, TCP: 6, TCP_LISTEN: 6)
Indicator	4 LEDs 1 Green/Red, Module Status (MOD) 1 Green/Red, Network Status (NET) 1 Green/Red, PLC Run/Stop Status (RUN) 1 Green/Red, Expansion I/O Module Status (IOS)

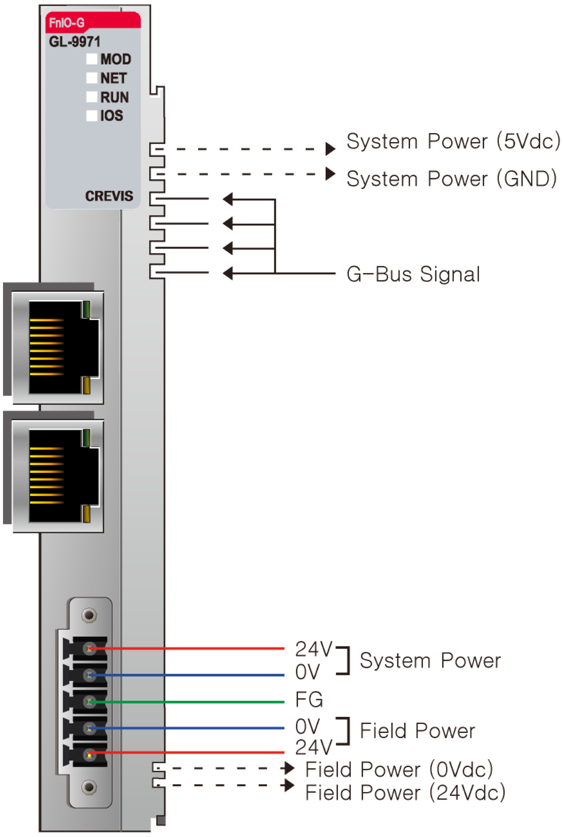
Ethernet Connection Specification	
Function	Max. Concurrent communications
Modbus/ TCP Master	1 Modbus TCP slaves can be connected
Modbus/ TCP Slave	6 Modbus TCP masters can be connected

*Field power range is dependent on I/O module series. Refer to I/O module's specification.

Specification

General Specification	
Power Dissipation	60mA typical @ 24Vdc
UL System Power	Supply voltage: 24Vdc nominal, Class 2
System Power	Supply voltage: 24Vdc nominal Supply voltage range: 15 ~ 28.8Vdc Reverse polarity protection
UL Field Power	Supply voltage: 24Vdc nominal, Class 2
Field Power*	Supply voltage: 24Vdc typical (Max. 30Vdc)
Max. Current Field Power Contact	Max. DC 8A
Wiring	I/O Cable Max. 2.0mm2(AWG 14)
Torque	0.8 Nm(7 lb-in)
Current for Expansion Module	1.0A @ 5Vdc
Isolation	System power to internal logic : Non-isolation System power I/O driver : Isolation
Max. Expansion Module	10 slots
I/O Data Size	Max. 128 Bytes each slot
Weight	76g
Module Size	109mm x 70mm x 22mm

2.2. Wiring Diagram

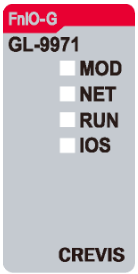


Pin No.	Signal Description	Signal Description	Pin No.
0	System Power, 24V	System Power, Ground	1
2	F.G	Field Power, Ground	3
4	Field Power, 24V	-	-

* **Warning:** The system power must not be connected with field power. Use seperate voltage supplies.

2.3. LED Indicator

2.3.1. LED Indicator



LED No.	LED Function / Description	LED Color
MOD	Module Status	Green/Red
NET	Network Status	Green/Red
RUN	PLC Status	Green/Red
IOS	Expansion IO Status	Green/Red

2.3.2. MOD (Module Status LED)

Status	LED is	To indicate
Not Powered	OFF	Power is not supplied to the unit.
Normal, Operational	Green	The unit is operating in normal condition.
IAP Mode*	Toggling Green & Red	Available for firmware download using FireFox.
Firmware Fault	Red	The unit has occurred unrecoverable fault in self-testing.
Recoverable Fault	Blinking Red	The unit has occurred recoverable fault in self-testing. - EEPROM checksum fault.

* The IP Address to access IAP web-server during IAP Mode: 192.168.100.10 (Recommended to use FireFox)

2.3.3. NET (Network Status LED)

Status	LED is	To indicate
Not Powered	OFF	Network off-line.
Link	Green	The LAN cable is physically connected to the ethernet port.

2.3.4. RUN (PLC Run/Stop Status LED)

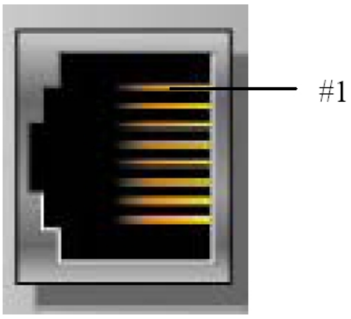
Status	LED is	To indicate
None PLC	OFF	Device has no program.
PLC Run	Green	PLC program is running.
PLC Stop	Blinking Green	PLC program stop.
Firmware Fault	Red	The unit has occurred unrecoverable fault in self-testing.
Diagnostic	Blinking Red	PLC program and expansion I/O modules do not match.

2.3.5. IOS LED (Expansion Module Status LED)

Status	LED is	To indicate
No Expansion I/O	OFF	Device has no expansion modules or not powered.
Have Expansion I/O	Green	Device has expansion modules.
Configuration Fault	Red	Replace expansion modules or fail to initialize. - Detect invalid expansion module ID. - Initial protocol failure. - Mismatch vendor code between adapter and expansion module. - Changed expansion module configuration.
Connection Fault	Blinking Red	One or more expansion module occurred in fault state. - Too many expansion modules. - Communication failure. - Overflowed I/O size.

2.4. Electrical Interface

2.4.1. RJ-45 Socket (2pcs)



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	

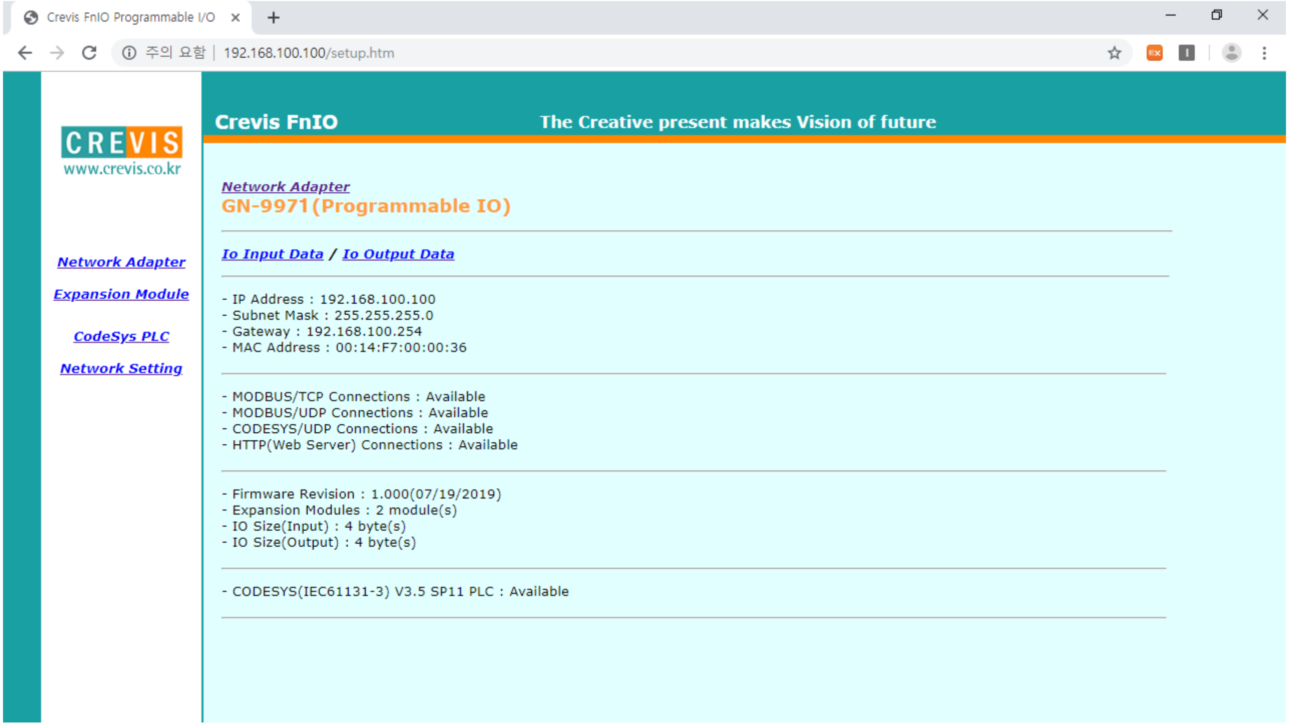
2.4.2. Toggle Switch and Push Botton

Toggle Switch Status	Module is	Description
UP	RUN	PLC Run
DOWN	STOP	PLC Stop

Push Botton	Module is	Description
Push and detach	Reset	Reset CodeSys PLC program and make the program be in the stop status.
Push for 5sec	PLC Reset	Erase CodeSys PLC program and retain memory.
Push for 20sec	Factory Reset	Erase CodeSys PLC program and parameter reset.
Push hold and Power Reset	IAP mode	Firmware download via FireFox.

2.5. Web-Server

*** Web-Server Address** : http://IP/setup.htm (http://192.168.100.100/setup.htm)



Crevis FnIO The Creative present makes Vision of future

Network Adapter
GN-9971(Programmable IO)

Io Input Data / Io Output Data

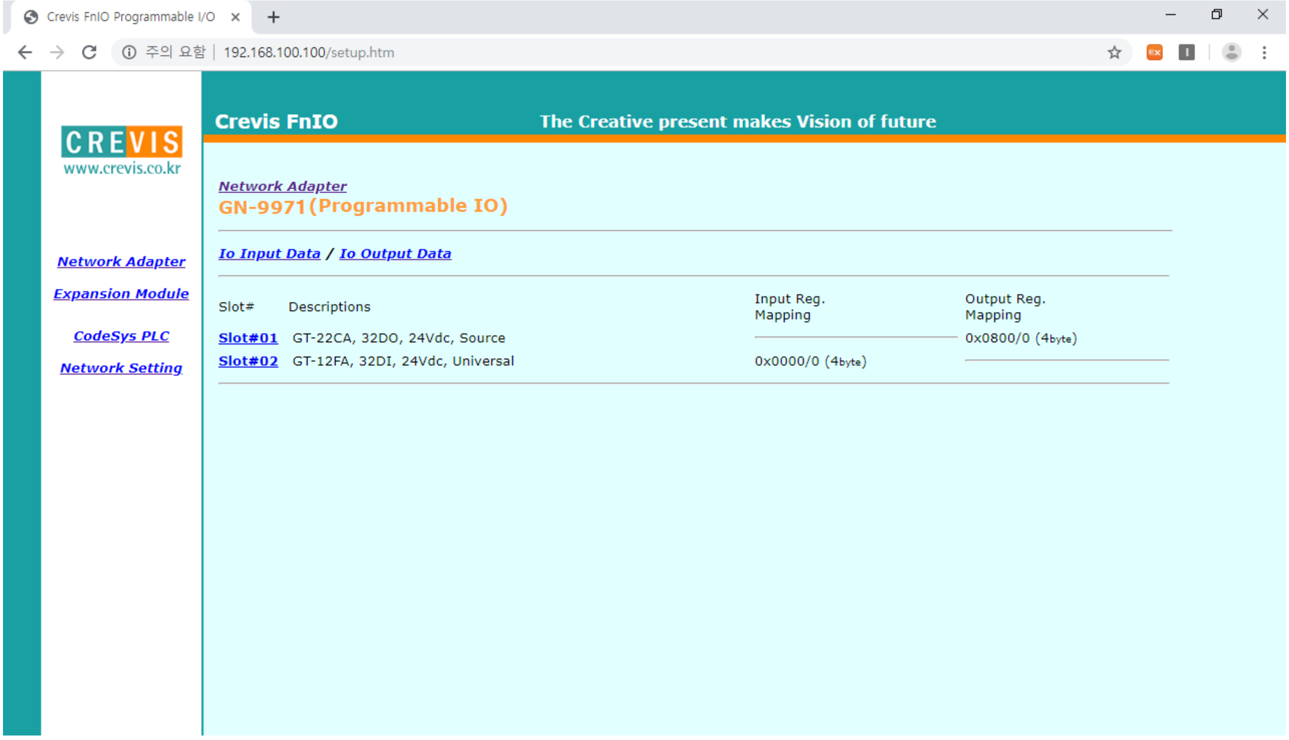
- IP Address : 192.168.100.100
- Subnet Mask : 255.255.255.0
- Gateway : 192.168.100.254
- MAC Address : 00:14:F7:00:00:36

- MODBUS/TCP Connections : Available
- MODBUS/UDP Connections : Available
- CODESYS/UDP Connections : Available
- HTTP(Web Server) Connections : Available

- Firmware Revision : 1.000(07/19/2019)
- Expansion Modules : 2 module(s)
- IO Size(Input) : 4 byte(s)
- IO Size(Output) : 4 byte(s)

- CODESYS(IEC61131-3) V3.5 SP11 PLC : Available

*** Expansion Module**: Provide the expansion modules that attatched to Network Adapter



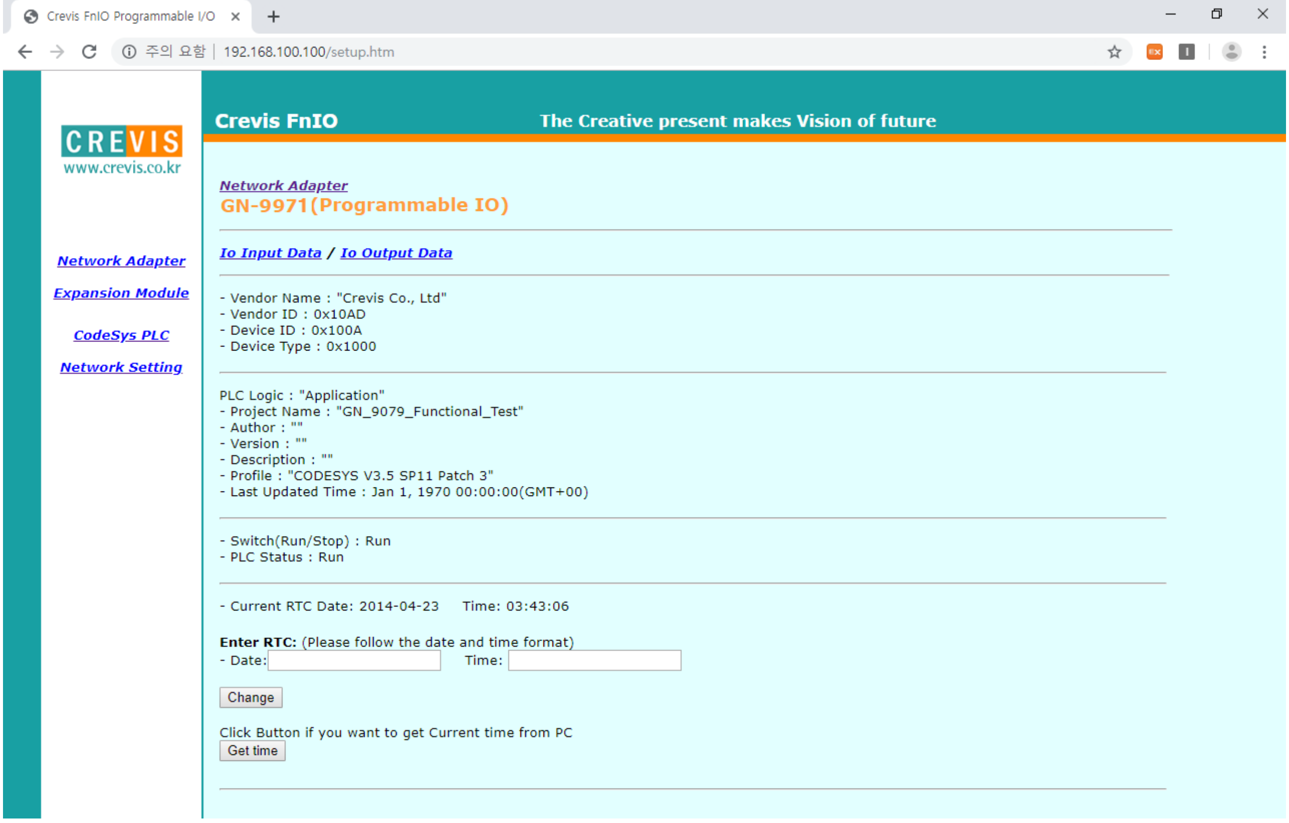
Crevis FnIO The Creative present makes Vision of future

Network Adapter
GN-9971(Programmable IO)

Io Input Data / Io Output Data

Slot#	Descriptions	Input Reg. Mapping	Output Reg. Mapping
Slot#01	GT-22CA, 32DO, 24Vdc, Source		0x0800/0 (4byte)
Slot#02	GT-12FA, 32DI, 24Vdc, Universal	0x0000/0 (4byte)	

* **CodeSys PLC**: Provide CodeSys PLC information and current RTC time. RTC time can be changeable in this page.


Crevis FnIO Programmable I/O
주의 요함 | 192.168.100.100/setup.htm
CREVIS
www.crevis.co.kr
Network Adapter
Expansion Module
CodeSys PLC
Network Setting
Crevis FnIO
The Creative present makes Vision of future

Network Adapter
GN-9971(Programmable IO)

Io Input Data / Io Output Data

- Vendor Name : "Crevis Co., Ltd"
- Vendor ID : 0x10AD
- Device ID : 0x100A
- Device Type : 0x1000

PLC Logic : "Application"
- Project Name : "GN_9079_Functional_Test"
- Author : ""
- Version : ""
- Description : ""
- Profile : "CODESYS V3.5 SP11 Patch 3"
- Last Updated Time : Jan 1, 1970 00:00:00(GMT+00)

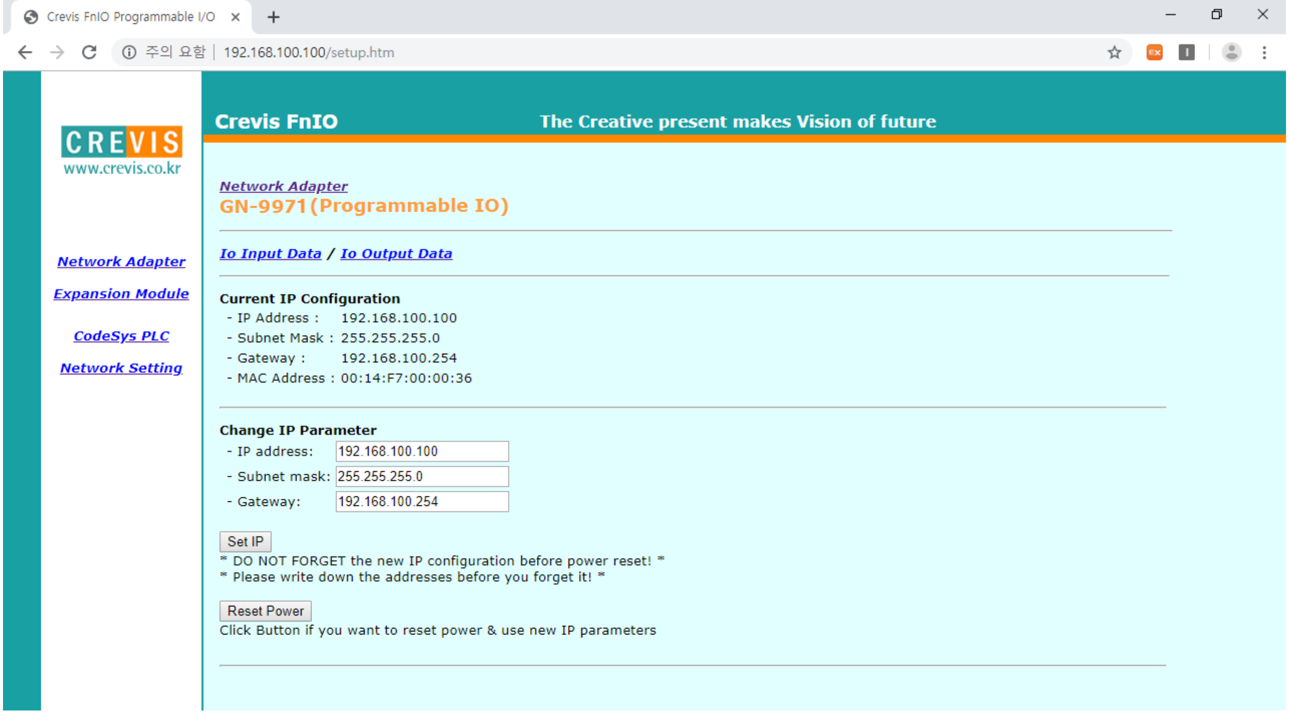
- Switch(Run/Stop) : Run
- PLC Status : Run

- Current RTC Date: 2014-04-23 Time: 03:43:06

Enter RTC: (Please follow the date and time format)
- Date: Time:

Click Button if you want to get Current time from PC

* **Network Setting**: Provide current IP configuration. IP parameter can change in this page.


Crevis FnIO Programmable I/O
주의 요함 | 192.168.100.100/setup.htm
CREVIS
www.crevis.co.kr
Network Adapter
Expansion Module
CodeSys PLC
Network Setting
Crevis FnIO
The Creative present makes Vision of future

Network Adapter
GN-9971(Programmable IO)

Io Input Data / Io Output Data

Current IP Configuration
- IP Address : 192.168.100.100
- Subnet Mask : 255.255.255.0
- Gateway : 192.168.100.254
- MAC Address : 00:14:F7:00:00:36

Change IP Parameter
- IP address: 192.168.100.100
- Subnet mask: 255.255.255.0
- Gateway: 192.168.100.254

* DO NOT FORGET the new IP configuration before power reset! *
* Please write down the addresses before you forget it! *

Click Button if you want to reset power & use new IP parameters

3. MODBUS/RTU INTERFACE

3.1. Surpported 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

3.1.1. (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.

3.1.2. (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.

3.1.3. (0x03) Read Holding Resgisters

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	0x01

- **Response**

Field name	Example
Function Code	0x03
Byte Count	0x04
Input Status	0x12
Input Status	0x34

- In case of address 0x0800, output register value: 0x1234.

3.1.4. (0x04) Read Input Resgisters

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	0x04
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.

3.1.5. (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.

3.1.6. (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.

3.1.7. (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+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, RS232/485 setting, and Bootp/DHCP mode will be the factory defaults value.

3) Mac Address will be the factory default value.

4) Refer to 3.2.2 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 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, Expansion Status

The response data field returns the status of ModBus and expansion addressed to the remote device.

This status values are identical with status 1word of input process image.

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

3.1.8. (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.

3.1.9. (0x10) Write Multiple Resgisters

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	0x10
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	0x10
Starting Address Hi	0x10
Starting Address Lo	0x08
Quantity of Registers Hi	0x00
Quantity of Registers Lo	0x02

.- In case of address 0x1008, 0x1009 output register value: 0x0000, 0x0000 changes to 0x1122, 0x3344.

3.1.10. (0x17) Read/Write Multiple Resgisters

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.

3.1.11. 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.
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.

- GL-9971 response exception code 01, 02, 03, 04 and 06.

3.2. 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).

3.2.1. Adapter Resgister Mapping

Address	IEC Address	Contents	Remarks
0x0000~0x07FF	%IW0~%IW2047	2048 words Input and Internal memory (Area is write-protected)	
0x0800~0x0FFF	%QW0~%QW2047	2048 words Output and Internal memory (Area is write-enabled)	
0x1000~0x1FFF	-	Special Function Register (PIO Information)	
0x2000~0x2FFF	-	Special Function Register (Slot Information)	
0x4000~0x5FFF	%MW0~%MW8191	8192 words Internal memory (Area is write-enabled)	

3.2.2. Adapter Identification Special Resgister (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 = 0x9160(GL-9971)
0x1003(4099)	Read	1word	Firmware revision, if 0x0101, revision 1.001
0x1005(4101)	Read	String upto 34bytes	Product name string First 1word is length of valid character string Example) response as following “00 0C 47 4C 2D 39 39 37 31 28 50 49 4F 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00” Valid character size = 0x000C = 12 characters "GL-9971(PIO)"
0x1006(4102)	Read	1word	Sum check of EEPROM
0x1010(4112)	Read	2words	Firmware release date
0x1013(4115)	Read	1word	Module ID = 0x9971(GL-9971)
0x101E(4126)	Read	15words	Composite Id of following address 0xA8C0(Lo_IP Addr),0x3264(Hi_IP Addr),0xFFFF(Lo_NetMask), 0x00FF(Hi_NetMask),0xA8C0(GateWay),0xFE64(GateWay), 0x1400(MacAddr),0x00F7(MacAddr),0xBA83(MacAddr), 0x02E5(VendorCode),0x000C(DeviceType),0x9120(ProductCode), 0x0200(FW_Rev),0x0420(FW_ReleasData),0x2018(FW_ReleasYear)

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

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

Address	Access	Type, Size	Description
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	1word	Run/Stop switch and Reset switch Stop : 0x0000 / Run : 0x0001 / Reset : 0x0002 ex) 0x0003 : Run + Reset Switch ON
0x110E(4366)	Read	upto 63words	Expansion slot's GT-number If the PIO is connected with GT-222F and GT-123F, then 0x222F 0x123F
0x1110(4368)	Read	1word	Number of expansion slot.
0x1113(4371)	Read	upto 11words	Expansion slot module id. First 1word is product code = 0x9160(GL-9971).
0x111E(4382)	Read	1word	Reserved. Adapter IO identification vendor code.

3.2.4. Adapter Setting Special Register (0x1600, 5632)

Address	Access	Type, Size	Description
0x1600(5632)	Read	2words	IP Address. (ex : A8C0 6464 = 192.168.100.100)
0x1602(5634)	Read	2words	Subnet Mask. (ex : FFFF 0000 = 255.255.0.0)
0x1604(5636)	Read	2words	Gate way. (ex : A8C0 0100 = 192.168.0.1)
0x160B(5643)	Read/Write	1word	IP Setting Method. - BootP/DHCP disable: 0x0000 - BootP : 0x8000 (default) - DHCP : 0x8001
0x1610(5648)	Read	3words	Mac Address (ex : 1400 00F7 0101 = 00.14.F7.00.01.01)
0x1620(5664)	Read/Write	4words	RTC - 1 word : 00ss (ss : sec) - 2 word : hhmm (hh : hour, mm : min) - 3 word : mmdd (mm : month, dd : day) - 4 word : yyyy (yyyy : year) (ex : 0010 0E19 0B1A 07E3 = 2019 - 11.26 - 14:25 - 16)

3.2.5. Expasion Slot Information Special Resister (0x2000, 8192)

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

Address Offset	Expansion Slot#1	Expansion Slot#2	Expansion Slot#3	Expansion Slot#4	……..	Expansion Slot#10
+ 0x00(+0)	0x2000(8192)	0x2020(8224)	0x2040(8256)	0x2060(8288)	…….	0x2120(8480)
+ 0x01(+1)	0x2001(8193)	0x2021(8225)	0x2041(8257)	0x2061(8289)	…….	0x2121(8481)
+ 0x02(+2)	0x2002(8194)	0x2022(8226)	0x2042(8258)	0x2062(8290)	…….	0x2122(8482)
+ 0x03(+3)	0x2003(8195)	0x2023(8227)	0x2043(8259)	0x2063(8291)	…….	0x2123(8483)
+ 0x04(+4)	0x2004(8196)	0x2024(8228)	0x2044(8260)	0x2064(8292)	…….	0x2124(8484)
+ 0x05(+5)	0x2005(8197)	0x2025(8229)	0x2045(8261)	0x2065(8293)	…….	0x2125(8485)
+ 0x06(+6)	0x2006(8198)	0x2026(8230)	0x2046(8262)	0x2066(8294)	…….	0x2126(8486)
+ 0x07(+7)	0x2007(8199)	0x2027(8231)	0x2047(8263)	0x2067(8295)	…….	0x2127(8487)
+ 0x08(+8)	0x2008(8200)	0x2028(8232)	0x2048(8264)	0x2068(8296)	…….	0x2128(8488)
+ 0x09(+9)	0x2009(8201)	0x2029(8233)	0x2049(8265)	0x2069(8297)	…….	0x2129(8489)
+ 0x0A(+10)	0x200A(8202)	0x202A(8234)	0x204A(8266)	0x206A(8298)	…….	0x212A(8490)
+ 0x0B(+11)	0x200B(8203)	0x202B(8235)	0x204B(8267)	0x206B(8299)	…….	0x212B(8491)
+ 0x0C(+12)	0x200C(8204)	0x202C(8236)	0x204C(8268)	0x206C(8300)	…….	0x212C(8492)
+ 0x0D(+13)	0x200D(8205)	0x202D(8237)	0x204D(8269)	0x206D(8301)	…….	0x212D(8493)
+ 0x0E(+14)	0x200E(8206)	0x202E(8238)	0x204E(8270)	0x206E(8302)	…….	0x212E(8494)
+ 0x0F(+15)	0x200F(8207)	0x202F(8239)	0x204F(8271)	0x206F(8303)	…….	0x212F(8495)
+ 0x10(+16)	0x2010(8208)	0x2030(8240)	0x2050(8272)	0x2070(8304)	…….	0x2130(8496)
+ 0x11(+17)	0x2011(8209)	0x2031(8241)	0x2051(8273)	0x2071(8305)	…….	0x2131(8497)
+ 0x12(+18)	0x2012(8210)	0x2032(8242)	0x2052(8274)	0x2072(8306)	…….	0x2132(8498)
+ 0x13(+19)	0x2013(8211)	0x2033(8243)	0x2053(8275)	0x2073(8307)	…….	0x2133(8499)
+ 0x14(+20)	0x2014(8212)	0x2034(8244)	0x2054(8276)	0x2074(8308)	…….	0x2134(8500)
+ 0x15(+21)	0x2015(8213)	0x2035(8245)	0x2055(8277)	0x2075(8309)	…….	0x2135(8501)
+ 0x16(+22)	0x2016(8214)	0x2036(8246)	0x2056(8278)	0x2076(8310)	…….	0x2136(8502)
+ 0x17(+23)	0x2017(8215)	0x2037(8247)	0x2057(8279)	0x2077(8311)	…….	0x2137(8503)
+ 0x18(+24)	0x2018(8216)	0x2038(8248)	0x2058(8280)	0x2078(8312)	…….	0x2138(8504)
+ 0x19(+25)	0x2018(8217)	0x2038(8249)	0x2058(8281)	0x2078(8313)	…….	0x2139(8505)
+ 0x1A(+26)	0x201A(8218)	0x203A(8250)	0x205A(8282)	0x207A(8314)	…….	0x213A(8506)
+ 0x1B(+27)	0x201B(8219)	0x203B(8251)	0x205B(8283)	0x207B(8315)	…….	0x213B(8507)
+ 0x1C(+28)	0x201C(8220)	0x203C(8252)	0x205C(8284)	0x207C(8316)	…….	0x213C(8508)
+ 0x1D(+29)	0x201D(8221)	0x203D(8253)	0x205D(8285)	0x207D(8317)	…….	0x213D(8509)
+ 0x1E(+30)	0x201E(8222)	0x203E(8254)	0x205E(8286)	0x207E(8318)	…….	0x213E(8510)
+ 0x1F(+31)	0x201F(8223)	0x203F(8255)	0x205F(8287)	0x207F(8319)	…….	0x213F(8511)

Address Offset	Access	Type, Size	Description
+ 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 word	Read input data this slot
+ 0x0B(+11)**	Read/Write	n word	Read/write output data this slot
+ 0x0E(+14)	Read	1 word	GT-number, if GT-22CA, returns 0x22CA
+ 0x0F(+15)	Read	String upto 72bytes	First 1word is length of valid character string. If GT-1238, returns "00 1E 52 54 2D 31 32 33 38 2C 20 38 44 49 2C 20 32 34 56 64 63 2C 20 55 6E 69 76 65 72 73 61 6C 00 00" Valid character size = 0x001E =30 characters, "GT-1238, 8DI, 24Vdc, Universal"
+ 0x10(+16)	Read	1 word	Size of configuration parameter byte
+ 0x11(+17)**	Read/Write	n word	Read/write Configuration parameter data, Refer to each IO parameter Specification.
+ 0x17(+23)	Read	2 words	Firmware Revision ex) 0x00010010 (Major revision 1 /Minor revision 16, Rev 1.016)
+ 0x19(+25)	Read	2 words	Firmware release data.

* 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.

3.3. Surpported MODBUS Function Codes

MODBUS Reference Documents

http://www.modubs.org

MODBUS Tools

http://www.modbustools.com, modbus poll

http://www.win-tech.com, modscan32