FnIO M - Series:

M9289

M9289 ETHERNET TCP/IP Network Adapter (Single Type)

Table of Contents

History

REV.	PAGES	REMARKS	DATE	Editor
-		Preliminary	2018/6/18	BS HA
1.00			2019/03/18	YM KIM
1.01	6,7,15	Vibration, Product changed, Added ATEX certification, M-Series caution	2020/05/20	CW SEO
1.02		Web server	2020/6/10	SA HWANG
1.03	38	Modify Firmware Revision	2020/10/29	CW SEO
1.04		Remove Description pages of Hot Swap Function, Use in Hazardous Environments and Caution(Before using the unit)	2020/12/7	SJ LIM
1.05	1,7,9,10	LINK led → D LINK changed	2020/12/23	CW SEO
1.06		Description changed(Modbus TCP/IP → Ethernet TCP/IP)	2021/08/06	CW SEO
1.07	6	Environment Specification Update	2021/11/16	EC KIM
1.08	6	Certificate Update	2023/06/01	CW SEO

1. ENVIRONMENT SPECIFICATION

Environmental specification	
Operating Temperature	-25℃~60℃
UL Temperature	-25℃~60℃
Storage Temperature	-40℃~85℃
Relative Humidity	5% ~ 90% non-condensing
Mounting	DIN rail
General specification	
Shock Operating	IEC 60068-2-27
Vibration Resistance	IEC 60068-2-6, 4g
Industrial Emissions	EN 61000-6-4/A11 : 2011
Industrial Immunity	EN 61000-6-2 : 2019
Installation Position	Vertical and horizontal installation is available.
Product Certifications	UL, ATEX, CE, UKCA, ABS, BV, CCS, DNV, KR, LR

2. M9289 (Ethernet TCP/IP NETWORK ADAPTER)

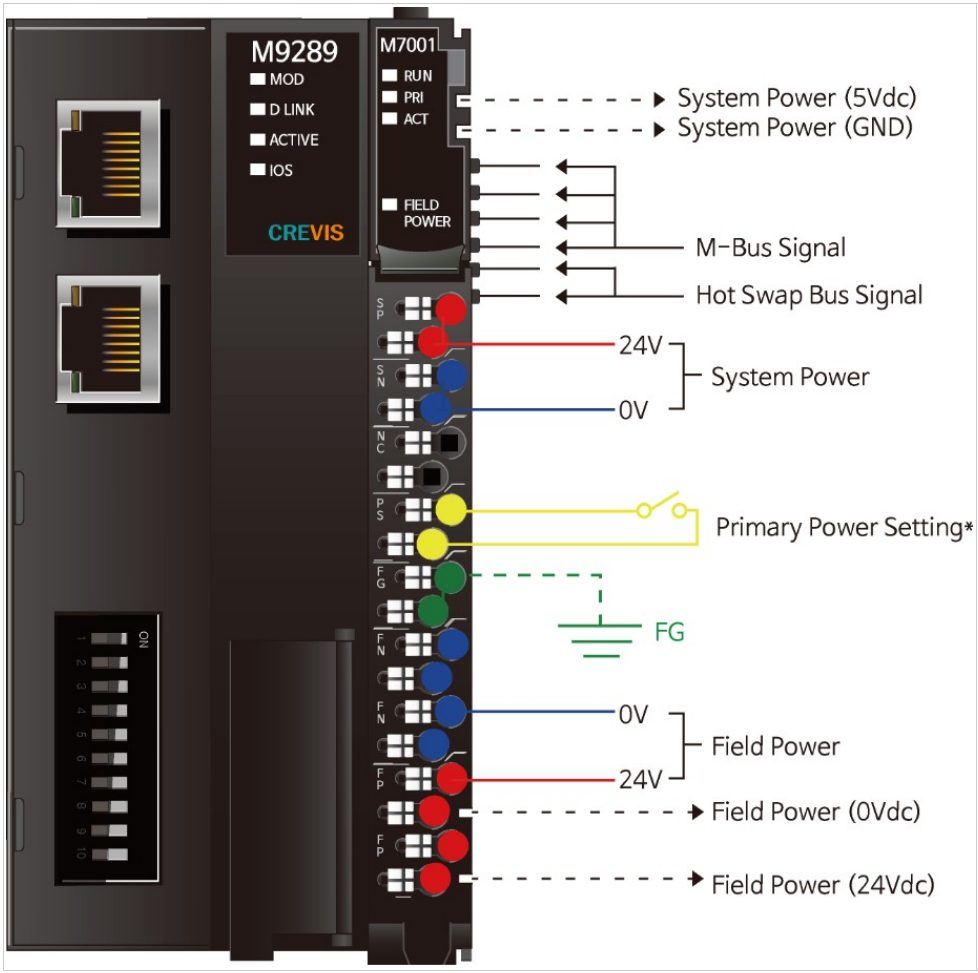
2.1. M9289 Specification

Items	Specification
Communication Interface Specification	
Adapter Type	Slave node (Ethernet TCP/IP), Single
Protocol	MODBUS/TCP,MODBUS/UDP,Ethernet/IP, CC-Link IE Field Basic
Sub-Protocol	HTTP,DHCP,10 TCP Connections, SLMP
Max. Expansion Module	63 slots
Modbus Max. Data Size(Input + Output)	Max 128 bytes each slot
Max Length Bus Line	Up to 100m from Ethernet Hub/Switch with twisted CAT5 UTP/STP
Max. Data Size(RX, RY)	each 32 bytes (4 Stations occupied)
Max. Data Size(RWr, RWw)	each 256 bytes (4 Stations occupied)
Max. link points per station (RX, RY)	each 64 points
Max. link points per station (RWr, RWw)	each 32 points
Max. Nodes	Limited by Ethernet Specification.
Baud Rate	10/100Mbps, Auto-negotiation, Full duplex
Interface Connector	RJ-45 socket * 2pcs
IP-Address Setup	Via DHCP/BOOTP or IOGuidePro(Crevis Software)
IP-Address Range	xxx.xxx.xxx.1 ~ 253 (User area)
IAP Mode	When DIP Switch 1 to 8 setting is 254 or 255 (Using only Internet Explorer / recommended version 11)
Serial Port	RS232 for MODBUS/RTU, Touch Pannel or IOGuidePro
Serial Configuration (RS232)	Node : 1 (Fixed) Baud Rate : 115200 (Fixed) Data bit : 8 (Fixed) Parity bit : No parity (Fixed) Stop bit : 1 (Fixed)
Indicator	4 LEDs 1 Green/Red, Module Status (MOD) 1 Green, Cyclic transmission status (D LINK) 1 Green, Exchange Data/Traffic Present LED (ACTIVE) 1 Green/Red, Expansion I/O Module Status (IOS) 2 LEDs (each RJ45 Connector) 1 Yellow, Link/Active 1 Green, Not used
Module Location	Starter module left side of M-Series system
General specification (Supplied by M7001)	
UL System Power	Supply voltage : 24Vdc nominal, Class 2
System Power	Supply voltage : 24Vdc nominal Supply voltage range : 15~28.8Vdc Protection : Output current limit, Reverse polarity protection
Power Dissipation	Network Adapter : 90mA typical @ 24Vdc
Current for I/O Module	2.0A @ 5Vdc (If except for NA, current for I/O module is about 1.5A)
Isolation	System power to internal logic : Non-isolation System power I/O driver : Isolation
UL Field Power	Supply voltage : 24Vdc nominal, Class 2
Field Power	Supply voltage : 24Vdc typical (Max.28.8Vdc) * Field Power Range is different depending on IO Module series. Refer to IO Module`s Specification.

Max. Current Field Power Contact	DC 10A Max
Torque	0.8Nm(7 lb-in)
Single Wire	0.205㎟ - 1.3㎟ (24-16 AWG)
Weight	179g
Module Size	54mm x 110mm x 75mm
Environment Condition	**Refer to '1. Environment Specification'**

* Class 2, adjacent to voltage rating (30Vmax)

2.2. M9289 Wiring Diagram



*** Primary Power Setting (P.S pin)**

- Short the P.S pin to set one of the two M7001 as the primary power.

Pin No.		Signal Description
0	SP	System Power, 24V
1	SP	System Power, 24V
2	SN	System Power, 0V(GND)
3	SN	System Power, 0V(GND)
4	NC	----------
5	NC	----------
6	PS	Primary Power Setting
7	PS	Primary Power Setting
8	FG	F.G
9	FG	F.G
10	FN	Field Power 0V (GND)
11	FN	Field Power 0V (GND)
12	FN	Field Power 0V (GND)
13	FN	Field Power 0V (GND)
14	FP	Field Power 24V
15	FP	Field Power 24V
16	FP	Field Power 24V
17	FP	Field Power 24V

Series No	Through Air	Over Surface	CTI
RTB18C	1.5mm	1.5mm	175≤CTI≤400

Spacings : The follwing minimum spcing in inches(millimeters) shall be maintained between uninsulated live parts of opposite polarity; and beween an uninsulated live part and a grounded Part including any mounting surface or exposed metal part.

2.3. M9289 LED Indicator

2.3.1. LED Indicator

LED No.	LED Function / Description	LED Color
MOD	Module Status	Green/Red
D LINK	Cyclic Transmission Status	Green
ACTIVE	Exchange Data/Traffic Present	Green
I/O	Extension Module Status	Green/Red

2.3.2. MOD (Module Status LED)

Status	LED	To indicate
Not Powered	OFF	Power is not supplied to the unit.
Device Operational	Green	The unit is operating in normal condition.
Unrecoverable Fault	Red	The device has an unrecoverable fault. - Memory error or CPU watchdog error.

2.3.3. D LINK (Cyclic transmission status LED)

Protocol	Status	LED	To indicate
CC-Link IE Field Basic	Disconnected	OFF	Disconnected
	Stop	Flashing Green	Cyclic transmission not being performed
	Run	Green	Cyclic transmission being performed

2.3.4. ACTIVE (Exchange Data/Traffic Present LED)

Protocol	Status	LED	To indicate
ModbusTCP	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.
Ethernet/IP	Not Powered No IP Address	OFF	Device does not have IP address or may not be powered
	CIP Connections	Green	Device has an IP address and at least one established connection.
	No Connections	OFF	Device has obtained an IP address, but has no established connections.
	Connection Time-out	Flashing Red	Connection time out in one or more of the connections the device has.

2.3.5. IOS LED (Extension Module Status LED)

Status	LED	To indicate
Not Powered	OFF	Device may not be powered.
Incorrect IO Module	Flashing Red	If Hotswap function is enable, configured module is incorrect.
Internal Bus Connection, Run Exchanging I/O	Green	Exchanging I/O data.
Expansion Configuration Failed	Red	One or more expansion module occurred in fault state. - Detected invalid expansion module ID. - Overflowed Input/Output Size - Too many expansion module - Internal Bus communication failure. - Initialization failure

		- Changed expansion module configuration. - Mismatch vendor code between adapter and expansion module.

2.4. M7001 LED Indicator

2.4.1. LED Indicator

LED No.	LED Function / Description	LED Color
RUN	M-Bus Status	Green
PRI	Primary Status	Green
ACT	Active	Green
Field Power	Field Power Enable	Green

2.4.2. RUN(RUN Status LED)

Status	LED	To indicate
Main Power Module	Green	Supplied 5Vdc system power.
Substitution Power Module	Off	Not Supplied 5Vdc system power.

2.4.3. PRI(Primary Status LED)

Status	LED	To indicate
Main Power Module	Green	Primary power module.
Substitution Power Module	Off	Secondary power module or not use redundancy function.

2.4.4. ACT(Active Status LED)

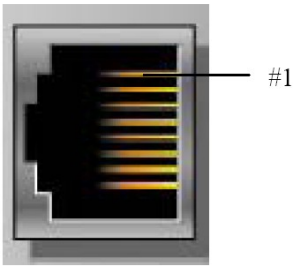
Status	LED	To indicate
Main Power Module	Green	When the Power Module is operating in main operation.
Substitution Power Module	Off	Standby with Substitution Power Module.

2.4.5. Field Power LED (Field Power Status LED)

Status	LED	To indicate
No field power	Off	Not supplied 24Vdc field power.
Supplied field power	Green	Supplied 24Vdc field power.

2.5. M9289 Electrical Interface

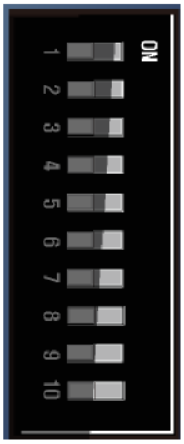
2.5.1. 5 Pin open connector



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

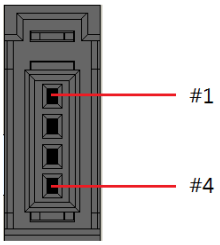
2.5.2. Dip Switch

*** Set Node 1~254**



DIP Pole#	Description	
1	IP_DIP bit#0	Lowest IP Address when Pole#10=ON ex) 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	
All On	IAP function (192.168.100.100)	

2.5.3. RS232 Port for MODBUS/RTU, Touch Panel or IO-Guide

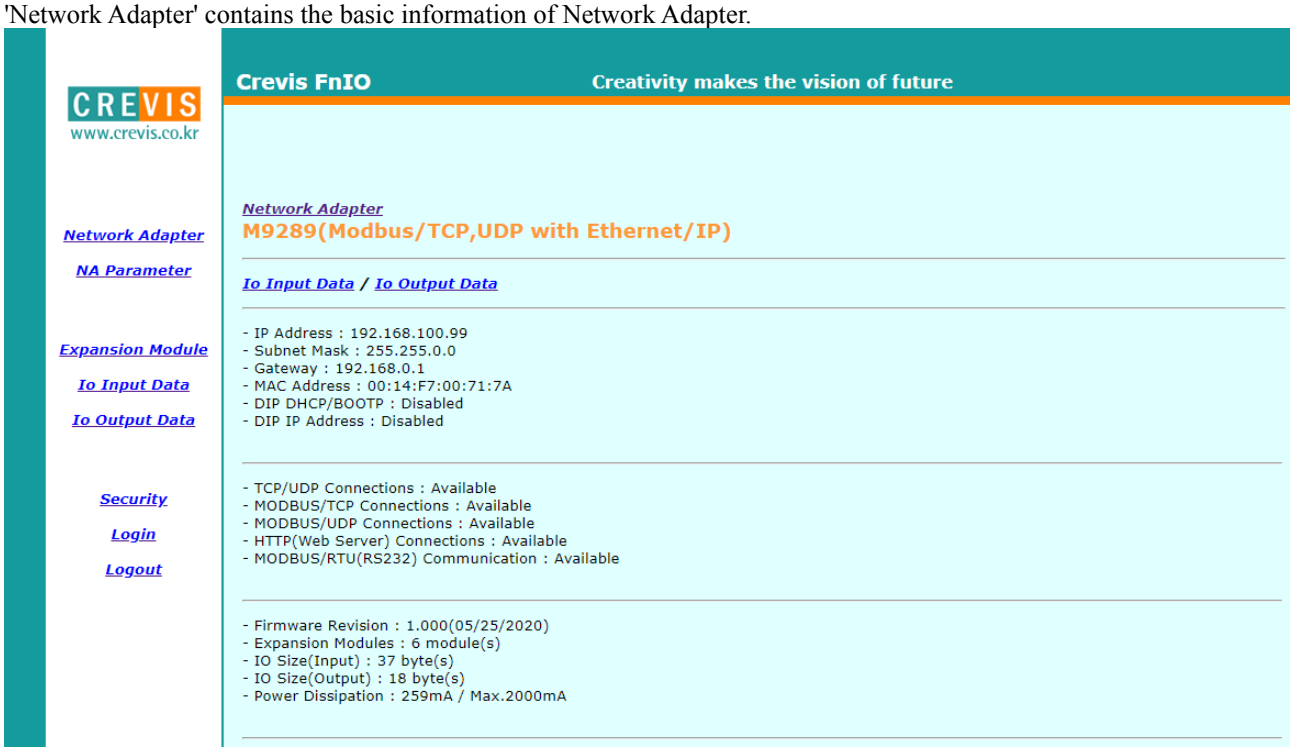


Pin#	Signal Name	Description
1	Reserved	----
2	TXD	RS232 TXD
3	RXD	RS232 RXD
4	GND	RS232 GND

2.6. MODBUS/TCP IP - Web Server

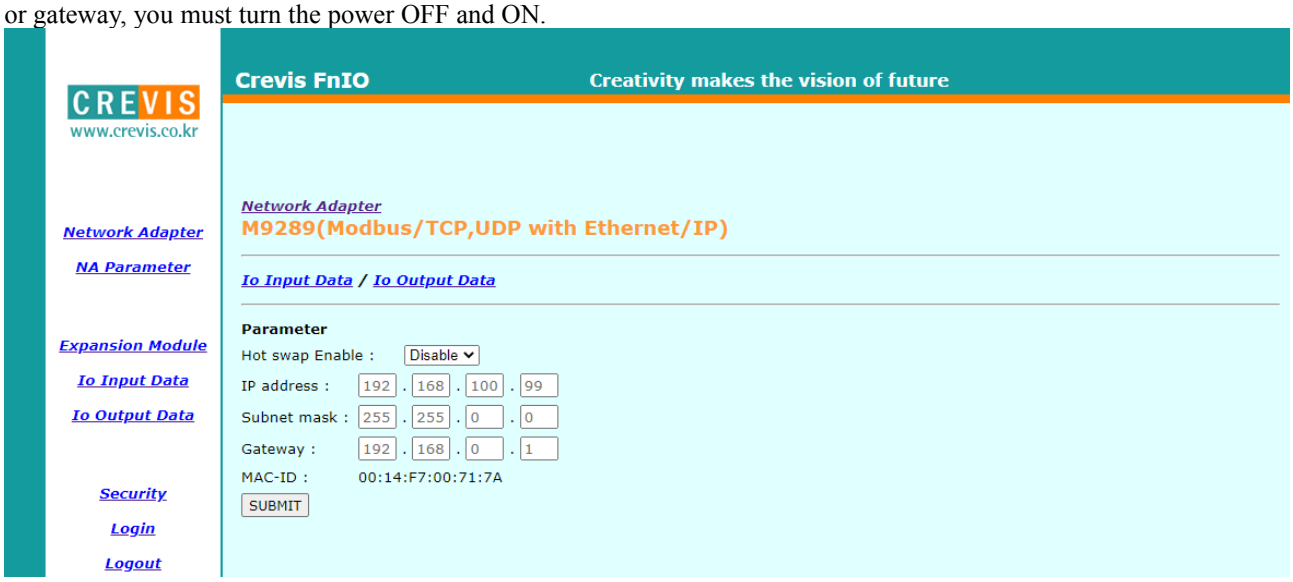
2.6.1. Network Adapter

'Network Adapter' contains the basic information of Network Adapter.



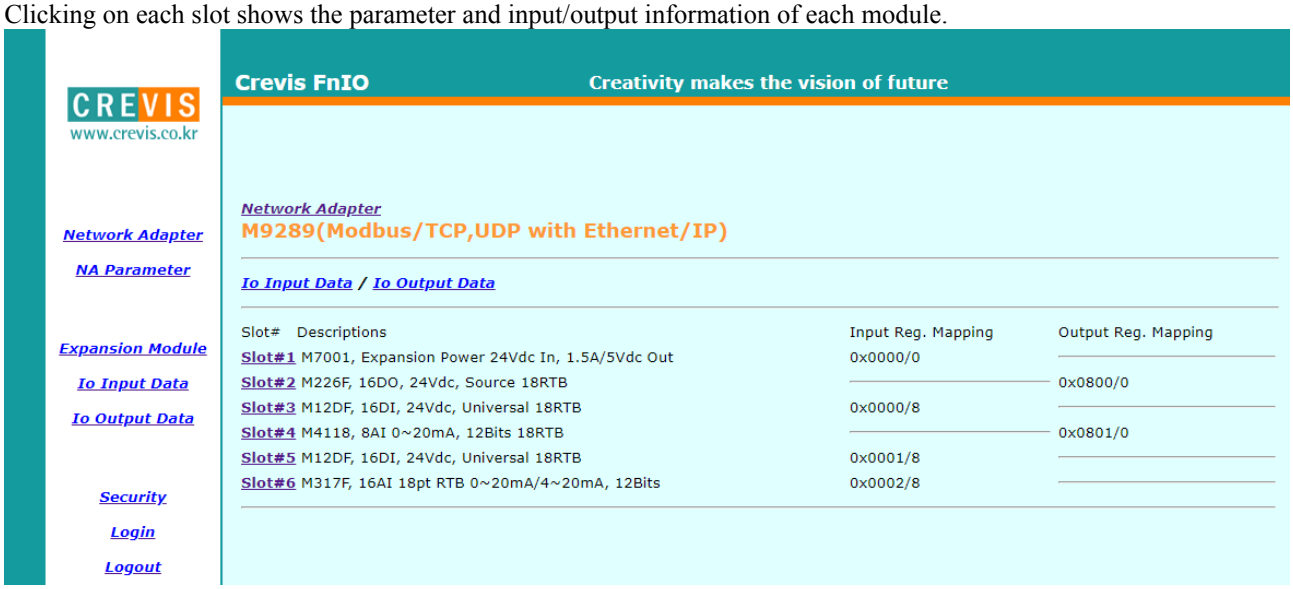
2.6.2. NA Parameter

Change the hotswap disable/enable and IP, subnet, gateway setting in 'NA Parameter'. When you change the IP, subnet or gateway, you must turn the power OFF and ON.

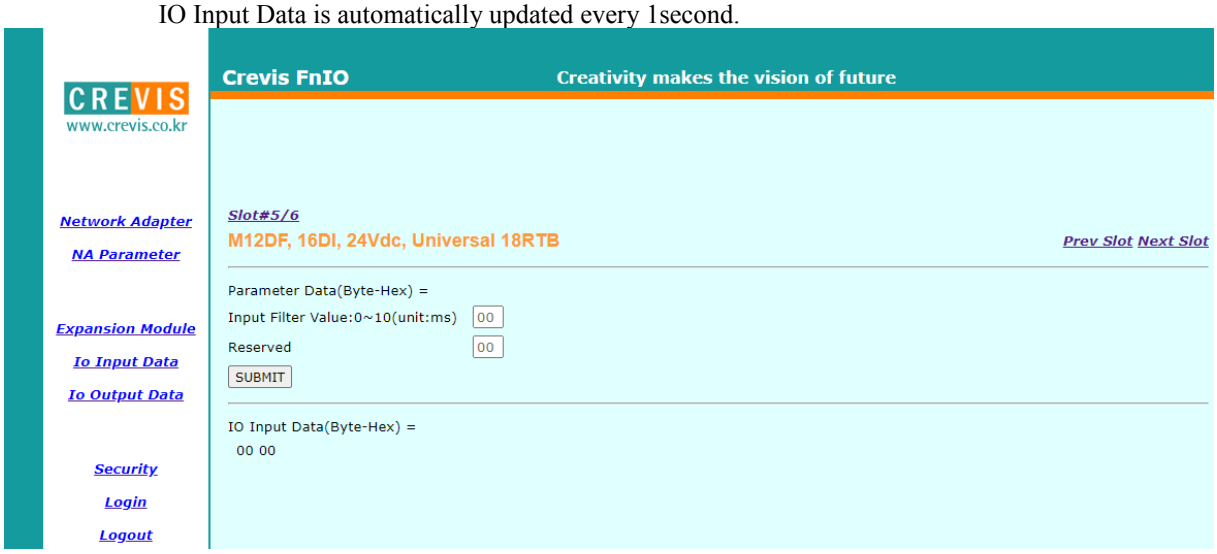


2.6.3. Expansion Module

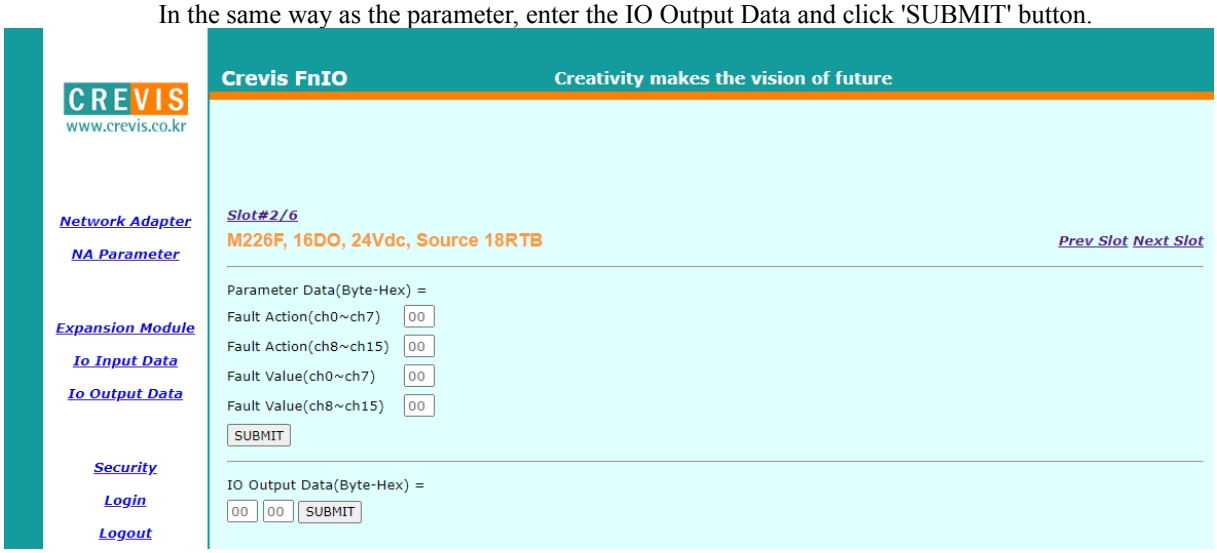
'Expansion Module' shows the expansion module connected to M9289.
Clicking on each slot shows the parameter and input/output information of each module.



Input Module : After entering the Parameter Data, click 'SUBMIT' button to change the parameter value.
IO Input Data is automatically updated every 1second.

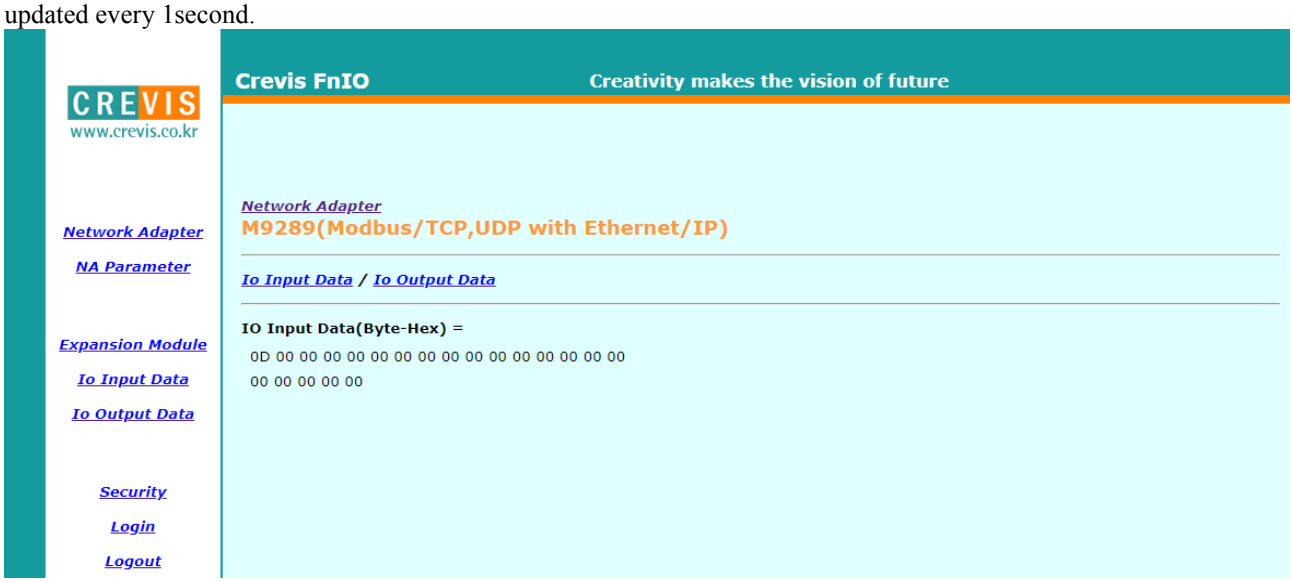


Output Module : After entering the Parameter Data, click 'SUBMIT' button to change the parameter value.
In the same way as the parameter, enter the IO Output Data and click 'SUBMIT' button.



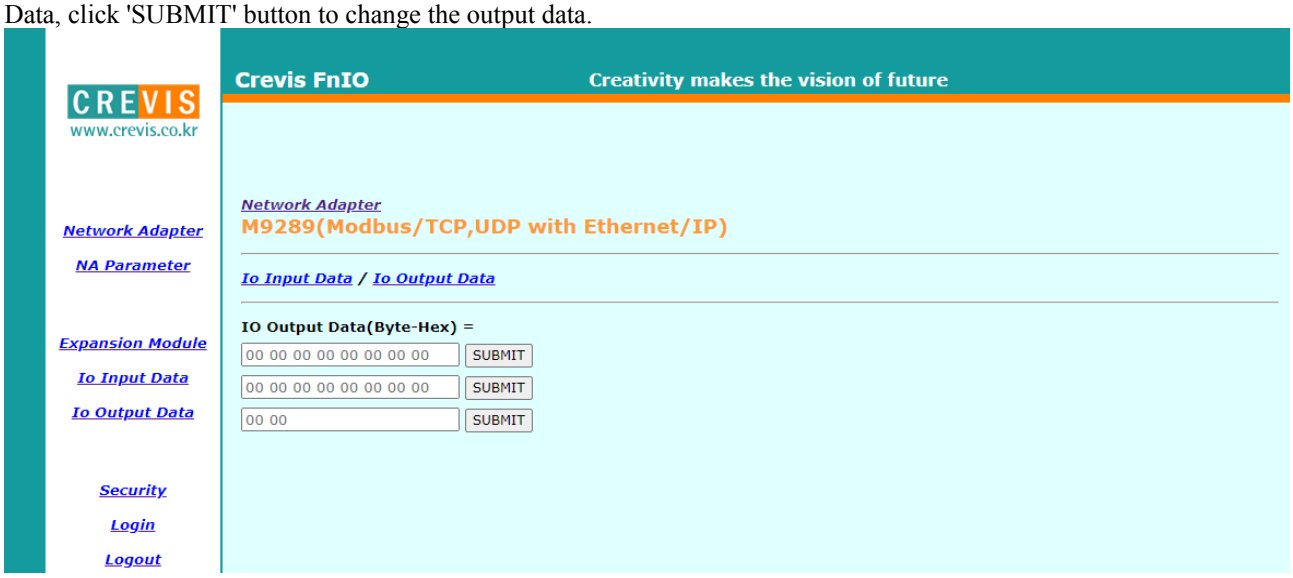
2.6.4. Io Input Data

In 'Io Input Data', all input data among the modules connected to M9289 are displayed. IO Input Data is automatically updated every 1second.



2.6.5. Io Output Data

In 'Io Output Data', all output data among the modules connected to M9289 are displayed. After entering the IO Output Data, click 'SUBMIT' button to change the output data.



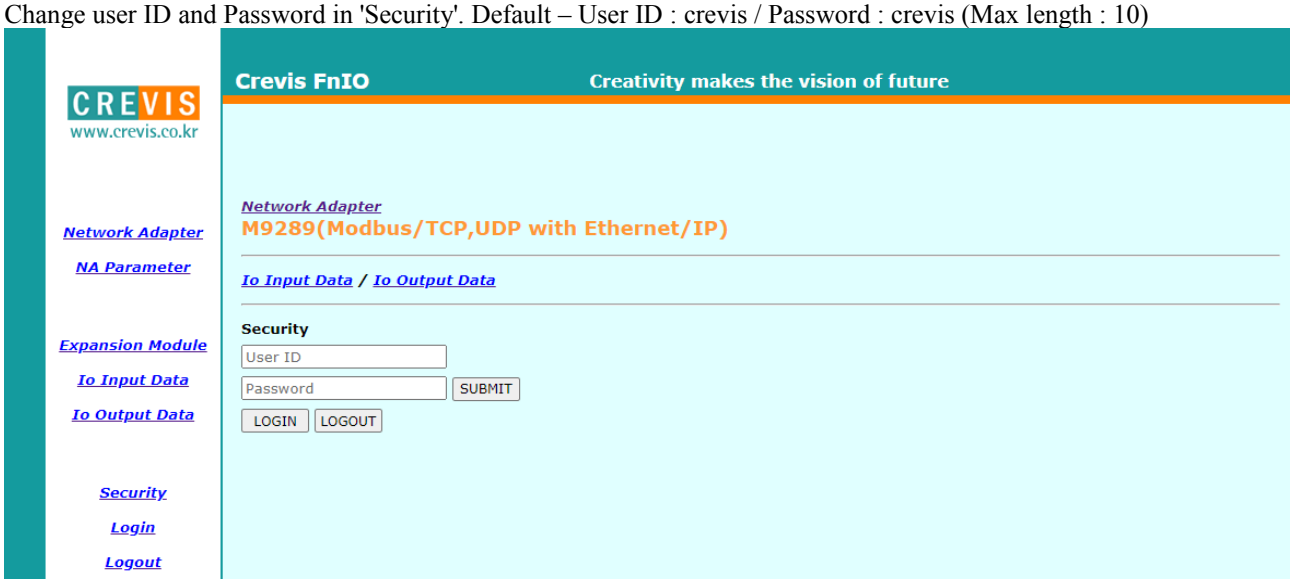
Output data is separated by spaces.
[Example]
- For explanation, it is marked with '/' instead of space.

NO	Write Data	Data Type	byte0	byte1	byte2	byte3	byte4	byte5	byte6	byte7
1)	/32/F/F0	Byte-Hex	0xXX	0x32	0x0F	0xF0	0xXX	0xXX	0xXX	0xXX
2)	A//F5/	Byte-Hex	0x0A	0xXX	0xF5	0xXX	0xXX	0xXX	0xXX	0xXX
3)	//14FC/A2/	Word-Hex	0xXX	0xXX	0xXX	0xXX	0xFC	0x14	0xA2	0x00
4)	EC/1045//D	Word-Hex	0xEC	0x00	0x45	0x10	0xXX	0xXX	0x0D	0x00

- No Changed : 0xXX

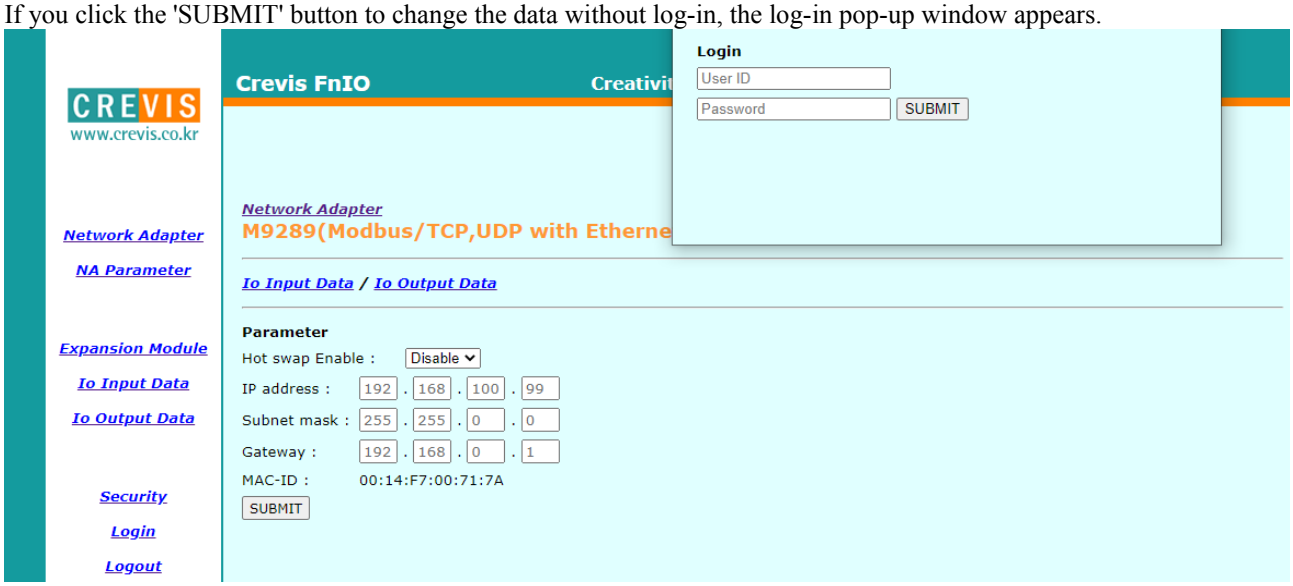
2.6.6. Security

Change user ID and Password in 'Security'. Default – User ID : crevis / Password : crevis (Max length : 10)



2.6.7. Log-in / Log-out

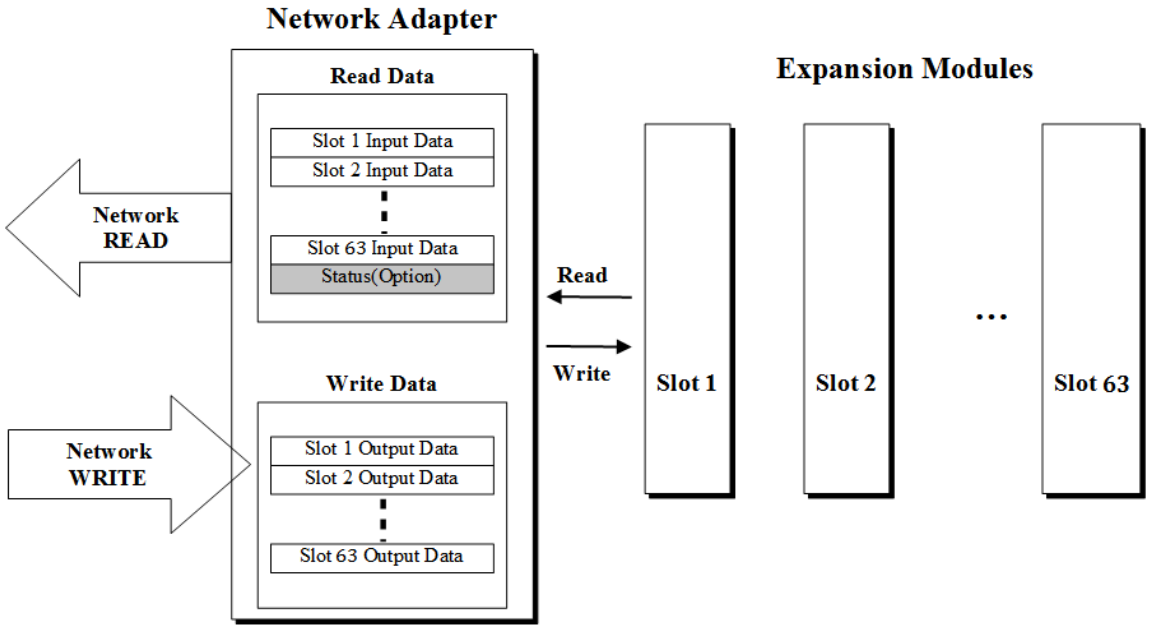
If you click the 'SUBMIT' button to change the data without log-in, the log-in pop-up window appears.



When you log-out, 'Log-out Success' pop-up appears.

2.7. 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 M-Series protocol. The following figure shows the data flow of process image between network adapter and expansion modules.



2.7.1. MODBUS Interface Register/Bit Map

- **Register Map**

Start Address	Read/Write	Description	Func. Code
0x0000 ~	Read	Process input image registers (Real Input Register)	3,4,23
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 each address (one address).

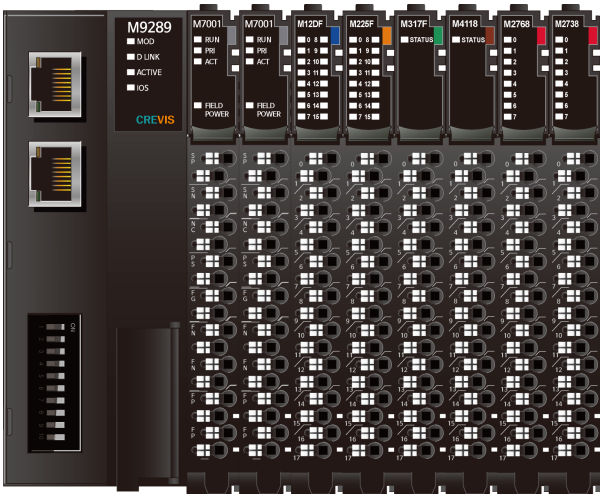
- **Register Map**

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

2.7.2. Example of Input and Output Process Image Map

Input image data depends on slot position and expansion slot data type. Input process image data is only ordered by expansion slot position

- **For example slot configuration**



Slot No.	Module Description
#0	MODBUS/TCP Adapter
#1	Power Input
#2	Power Input
#3	16-discrete input
#4	16-discrete output
#5	16-analog input
#6	8-analog output
#7	8-discrete output
#8	8-discrete output

- **Input Process Image**

Address	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
0x0000	Power Input (Slot#2)								Power Input (Slot#1)							
0x0001	Discrete Input 16 pts (Slot#3)															
0x0002	Analog Input Ch0 high byte (Slot#5)								Analog Input Ch0 low byte (Slot#5)							
0x0003	Analog Input Ch1 high byte (Slot#5)								Analog Input Ch1 low byte (Slot#5)							
0x0004	Analog Input Ch2 high byte (Slot#5)								Analog Input Ch2 low byte (Slot#5)							
0x0005	Analog Input Ch3 high byte (Slot#5)								Analog Input Ch3 low byte (Slot#5)							
0x0006	Analog Input Ch4 high byte (Slot#5)								Analog Input Ch4 low byte (Slot#5)							
0x0007	Analog Input Ch5 high byte (Slot#5)								Analog Input Ch5 low byte (Slot#5)							
0x0008	Analog Input Ch6 high byte (Slot#5)								Analog Input Ch6 low byte (Slot#5)							
0x0009	Analog Input Ch7 high byte (Slot#5)								Analog Input Ch7 low byte (Slot#5)							
0x000A	Analog Input Ch8 high byte (Slot#5)								Analog Input Ch8 low byte (Slot#5)							
0x000B	Analog Input Ch9 high byte (Slot#5)								Analog Input Ch9 low byte (Slot#5)							
0x000C	Analog Input Ch10 high byte (Slot#5)								Analog Input Ch10 low byte (Slot#5)							
0x000D	Analog Input Ch11 high byte (Slot#5)								Analog Input Ch11 low byte (Slot#5)							
0x000E	Analog Input Ch12 high byte (Slot#5)								Analog Input Ch12 low byte (Slot#5)							
0x000F	Analog Input Ch13 high byte (Slot#5)								Analog Input Ch13 low byte (Slot#5)							
0x0010	Analog Input Ch14 high byte (Slot#5)								Analog Input Ch14 low byte (Slot#5)							
0x0011	Analog Input Ch15 high byte (Slot#5)								Analog Input Ch15 low byte (Slot#5)							

- **Output Process Image**

Address	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
0x0800	Discrete Output 16 pts (Slot#4)															
0x0801	Analog Output Ch0 high byte (Slot#6)								Analog Output Ch0 low byte (Slot#6)							
0x0802	Analog Output Ch1 high byte (Slot#6)								Analog Output Ch1 low byte (Slot#6)							
0x0803	Analog Output Ch2 high byte (Slot#6)								Analog Output Ch2 low byte (Slot#6)							
0x0804	Analog Output Ch3 high byte (Slot#6)								Analog Output Ch3 low byte (Slot#6)							
0x0805	Analog Output Ch4 high byte (Slot#6)								Analog Output Ch4 low byte (Slot#6)							
0x0806	Analog Output Ch5 high byte (Slot#6)								Analog Output Ch5 low byte (Slot#6)							
0x0807	Analog Output Ch6 high byte (Slot#6)								Analog Output Ch6 low byte (Slot#6)							
0x0808	Analog Output Ch7 high byte (Slot#6)								Analog Output Ch7 low byte (Slot#6)							
0x0809	Discrete Output 8 pts (Slot#8)								Discrete Output 8 pts (Slot#7)							

3. MODBUS INTERFACE

3.1. MODBUS Interface Register/Bit Map

- **Register Map**

Start Address	Read/Write	Description	Func. Code
0x0000 ~	Read	Process input image registers (Real Input Register)	3,4,23
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 each address (one address).

- **Register Map**

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

3.2. Supported MODBUS Function Codes

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

- Refer to MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1a

3.3. MODBUS Transmission Mode

Two different serial transmission modes are defined : The RTU mode and the ASCII mode. It defines the bit contents of message fields transmitted serially on the line. It determines how information is packed into the message fields and decoded.

3.3.1. RTU Transmission Mode

When devices communicate on a MODBUS serial line using the RTU (Remote Terminal Unit) mode, each 8–bit byte in a message contains two 4–bit hexadecimal characters. The main advantage of this mode is that its greater character density allows better data throughput than ASCII mode for the same baud rate. Each message must be transmitted in a continuous stream of characters.

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

3.3.2. 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	RTU
Start of Frame	-	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x01	0x01
Starting Address Hi	0x10	0x10
Starting Address Lo	0x00	0x00
Quantity of Outputs Hi	0x00	0x00
Quantity of Outputs Lo	0x10	0x10
Error Check (CRC/LRC)	-	0x31, 0x44
End of Frame	-	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x01	0x01
Byte Count	0x02	0x02
Output Status	0x00	0x00
Output Status	0x00	0x00
Error Check (CRC/LRC)	---	0x40, 0x34
End of Frame	---	t1-t2-t3

3.3.3. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x02	0x02
Starting Address Hi	0x00	0x00
Starting Address Lo	0x00	0x00
Quantity of Inputs Hi	0x00	0x00
Quantity of Inputs Lo	0x10	0x10
Error Check (CRC/LRC)	---	0x71, 0x84
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x02	0x02
Byte Count	0x02	0x02
Input Status	0x00	0x00
Input Status	0x00	0x00
Error Check (CRC/LRC)	---	0x40, 0x70
End of Frame	---	t1-t2-t3

3.3.4. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x03	0x03
Starting Address Hi	0x10	0x10
Starting Address Lo	0x00	0x00
Quantity of Register Hi	0x00	0x00
Quantity of Register Lo	0x01	0x01
Error Check (CRC/LRC)	---	0x88, 0x88
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x03	0x03
Byte Count	0x02	0x02
Output Register#0 Hi	0x02	0x02
Output Register#0 Lo	0xE5	0xE5
Error Check (CRC/LRC)	---	0x81, 0x67
End of Frame	---	t1-t2-t3

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

3.3.5. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x04	0x04
Starting Address Hi	0x10	0x10
Starting Address Lo	0x00	0x00
Quantity of Register Hi	0x00	0x00
Quantity of Register Lo	0x01	0x01
Error Check (CRC/LRC)	---	0x3D, 0x48
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3

Slave Address	0x63	0x63
Function Code	0x04	0x04
Byte Count	0x02	0x02
Input Register#0 Hi	0x02	0x02
Input Register#0 Lo	0xE5	0xE5
Error Check (CRC/LRC)	---	0x80, 0x13
End of Frame	---	t1-t2-t3

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

3.3.6. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x05	0x05
Output Address Hi	0x10	0x10
Output Address Lo	0x00	0x00
Output Value Hi	0xFF	0xFF
Output Value Lo	0x00	0x00
Error Check (CRC/LRC)	---	0x80, 0xB8
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x05	0x05
Output Address Hi	0x10	0x10
Output Address Lo	0x00	0x00
Output Value Hi	0xFF	0xFF
Output Value Lo	0x00	0x00
Error Check (CRC/LRC)	---	0x80, 0xB8
End of Frame	---	t1-t2-t3

- Output bit of address 0x1001 turns ON.

3.3.7. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x06	0x06
Register Address Hi	0x08	0x08
Register Address Lo	0x00	0x00
Register Value Hi	0x00	0x00
Register Value Lo	0xFF	0xFF
Error Check (CRC/LRC)	---	0xC3, 0xA8
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x06	0x06
Register Address Hi	0x08	0x08
Register Address Lo	0x00	0x00
Register Value Hi	0x00	0x00

Register Value Lo	0xFF	0xFF
Error Check (CRC/LRC)	---	0xC3, 0xA8
End of Frame	---	t1-t2-t3

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

3.3.8. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x07	0x07
Function Code	0x08	0x08
Sub-Function Hi	0x00	0x00
Sub-Function Lo	0x00	0x00
Data Hi	0x11	0x11
Data Lo	0x22	0x22
Error Check (CRC/LRC)	---	0x6C, 0x24
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x07	0x07
Function Code	0x08	0x08
Sub-Function Hi	0x00	0x00
Sub-Function Lo	0x00	0x00
Data Hi	0x11	0x11
Data Lo	0x22	0x22
Error Check (CRC/LRC)	---	0x6C, 0x24
End of Frame	---	t1-t2-t3

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+0xAB7B+Sumcheck	Echo Request Data	Reset with Factory default [1]
0x0001(1)	0x55AA+0xAA55+Sumcheck	Echo Request Data	Reset with Factory default [2]

1) Watchdog time value, auto recovery will be the factory defaults value.
2) Mac Address, IP Address, Subnet Mask Address, Gateway Address will be the factory defaults value.

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

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

Sub-function 0x000B(11) Return Bus Message Count
The response data field returns the quantity of messages that the remote device has detected on the communications

system since its last restart, clear counters operation, or power–up.

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

Sub-function 0x000C(12) Return Bus Communication Error Count

The response data field returns the quantity of CRC errors encountered by the remote device since its last restart, clear counters operation, or power–up.

Sub-function	Data Field (Request)	Data Field (Response)	Description
0x000C(12)	0x0000	CRC Error 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, Internal Bus Status

The response data field returns the status of ModBus and Internal Bus 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, Internal Bus Status	Same as status 1word

Sub-function 0x0065(101) Return Slave Watchdog Error Count

The response data field returns the quantity of watchdog error addressed to the remote device since its last restart, clear counters operation, or power–up.

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

3.3.9. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x0F	0x0F
Starting Address Hi	0x10	0x10
Starting Address Lo	0x00	0x00
Quantity of Outputs Hi	0x00	0x00
Quantity of Outputs Lo	0x10	0x10
Byte Count	0x02	0x02
Output Value#0	0x0F	0x0F
Output Value#1	0x00	0x00
Error Check (CRC/LRC)	---	0x47, 0x73
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x0F	0x0F
Starting Address Hi	0x10	0x10
Starting Address Lo	0x00	0x00
Quantity of Outputs Hi	0x00	0x00
Quantity of Outputs Lo	0x10	0x10
Error Check (CRC/LRC)	---	0x58, 0x85
End of Frame	---	t1-t2-t3

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

3.3.10. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x10	0x10
Starting Address Hi	0x08	0x08
Starting Address Lo	0x00	0x00
Quantity of Registers Hi	0x00	0x00
Quantity of Registers Lo	0x01	0x01
Byte Count	0x02	0x02
Register Value#0 Hi	0x00	0x00
Register Value#0 Lo	0xFF	0xFF
Error Check (CRC/LRC)	---	0xDE, 0xB2
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x10	0x10
Starting Address Hi	0x08	0x08
Starting Address Lo	0x00	0x00
Quantity of Registers Hi	0x00	0x00
Quantity of Registers Lo	0x01	0x01
Error Check (CRC/LRC)	---	0x0B, 0xEB
End of Frame	---	t1-t2-t3

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

3.3.11. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x17	0x17
Read Starting Address Hi	0x00	0x00
Read Starting Address Lo	0x00	0x00
Quantity of Read Hi	0x00	0x00

Quantity of Read Lo	0x01	0x01
Write Starting Address Hi	0x08	0x08
Write Starting Address Lo	0x00	0x00
Quantity of Write Hi	0x00	0x00
Quantity of Write Lo	0x01	0x01
Byte Count	0x02	0x02
Write Reg. Value#0 Hi	0x00	0x00
Write Reg. Value#0 Lo	0xFF	0xFF
Error Check (CRC/LRC)	---	0x1B, 0xCC
End of Frame	---	t1-t2-t3

- **Response**

Field name	Example	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x63	0x63
Function Code	0x17	0x17
Byte Count	0x02	0x02
Read Reg. Value#0 Hi	0x00	0x00
Read Reg. Value#0 Lo	0xFF	0xFF
Error Check (CRC/LRC)	---	0x04, 0x3C
End of Frame	---	t1-t2-t3

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

3.3.12. 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	RTU
Start of Frame	---	t1-t2-t3
Slave Address	0x07	0x07
Function Code	0x81	0x81
Exception Code	0x02	0x02
Error Check (CRC/LRC)	---	0x22, 0xC0
End of Frame	---	t1-t2-t3

- **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.

- M9289 response exception code 01, 02, 03, 04 and 06.

3.4. 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 each address (one address).

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

Address	Access	Type, Size	Description
0x1000(4096)	Read	1word	Vendor ID = 0x02E5(741), Crevis. Co., Ltd.
0x1001(4097)	Read	1word	Device type = 0x000C, Network Adapter
0x1002(4098)	Read	1word	Product Code = 0xA000
0x1003(4099)	Read	1word	Firmware revision, if 0x0101, revision 1.01
0x1004(4100)	Read	2word	Product unique serial number
0x1005(4101)	Read	String upto 36byte	Product name string (ASCII) “M9289,ETHERNET TCP/IP Adapter,MBUS”
0x1006(4102)	Read	1word	Sum check of EEPROM
0x1010(4112)	Read	2word	Firmware release date
0x1011(4113)	Read	2word	Product manufacturing inspection date
0x101E(4126)	Read	 7word - 1word - 1word - 1word - 1word - 1word - 2word 15word - 2word - 2word - 2word - 3word - 1word - 1word - 1word - 1word - 2word	Composite Id of following address * RTU mode 0x1100(4352), Modbus RS232 Node. (Fixed 0x0001) 0x1000(4096), Vendor ID 0x1001(4097), Device type 0x1002(4098), Product code 0x1003(4099), Firmware revision 0x1004(4100), Product serial number *TCP mode 0x1050(4176), IP address 0x1051(4177), Subnet mask 0x1052(4178), Gateway 0x1053(4179), Ethernet physical address (MAC ID) 0x1000(4096), Vendor ID 0x1001(4097), Device type 0x1002(4098), Product code 0x1003(4099), Firmware revision 0x1004(4100), Product serial number

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

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

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

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

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

Address	Access	Type, Size	Description
0x1040(4160)	Read	1word	Reserved
0x1041(4161)	Read/Write	1word	MODBUS/TCP connection timeout time. (0.5sec unit) Maximum time of ModBus connection to stay to be opened without receiving a ModBus request. 0~3600 The 120 (60sec) is default value. The value 0 disables connection time out specially.
0x1042(4162)	Read	1word	Number of ModBus/TCP connected
0x1043(4163)	Read	1word	ModBus/TCP port, fixed 502
0x1044(4164)	Read	1word	Ethernet Interface Speed, 10(10Mbps) or 100(100Mbps)
0x1045(4165)*	Read/Write	1word	IP Setting Method. 0: BOOTP, 1:DHCP
0x1046(4166)	---	---	Reserved.
0x1047(4167)	Read	1word	Status of DIP SW#9 DHCP/BOOTP(Enable/Disable). 0 : OFF, 1 : ON
0x1048(4168)	Read	1word	Enable/disable Lowest IP address via DIP Switch, 1:Enabled
0x1050(4176)	Read/Write	2word	IP address. If 192.168.123.1, then 0xA8C0, 0x017B. After update this value, IP address, Subnet mask and Gateway are applied as new one.
0x1051(4177)	Read/Write	2word	Subnet mask. If 255.255.255.0, then 0xFFFF, 0x00FF.
0x1052(4178)	Read/Write	2word	Gateway. If 192.168.123.254, then 0xA8C0, 0xFE7B.
0x1053(4179)	Read	3word	Ethernet physical address (MAC-ID). If 11-22-33-44-55-66, then 0x2211, 0x4433, 0x6655.

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

3.4.4. Adapter Hotswap Register (0x1060, 4192)

Address	Access	Type, Size	Description
0x1060(4192)	Read/ Write	1word	Hot swap Disable 0 : Enable 1 : Disable
0x1062(4194)*	Read	1word	Error slot detection 0 : No error slot 1 : Error slot detection
0x1063(4195)*	Read	4word	Error slot location, 8x8 bit

* 0x1062 and 0x1063 functions are only available if hot swap(0x1060) is enabled.

3.4.5. Adapter Connection Network Register (0x1080, 4224)

Address	Access	Type, Size	Description
0x1080(4224)*	Read/ Write	1word	Protocol connection information - O : Cyclic Output refresh and Master fault action Enable - X : Cyclic Output refresh and Master fault action Disable (Acyclic Output, Cyclic input, Parameter Enable)
0x1081(4225)	Read	1word	Ethernet IP connection status 1 : Power on status 2 : Connection 4 : Disconnection
0x1082(4226)	Read	1word	CC-Link IE Field Basic connection status 0 : Disconnection 1 : Master STOP Connection 2 : Master RUN Connection

Value		Modbus	Ethernet I/P	CC-Link IEF	Future use
	0x0	O	O	O	X
0x9	0x1	O	X	X	X
0xA	0x2	X	O	X	X
0xB	0x3	O	O	X	X
0xC	0x4	X	X	O	X
0xD	0x5	O	X	O	X
0xE	0x6	X	O	O	X
0xF	0x7	O	O	O	X
	0x8	X	X	X	X

* Factory default value is 0x0f
* if set to 0, the value is set to 0x0f and read.
* It is recommended to use one protocol per node for minimize communication traffic.

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

<table>
<tr><th>Address</th><th>Access</th><th>Type, Size</th><th>Description</th></tr>
<tr><td>0x1100(4352)*</td><td>Read/Write</td><td>1word</td><td>Master fault action option. (Disable : 0x0000, Enable : 0x0001)
This option can enable Master fault action option.
With master fault action, fault action can be activated with master communication failure. Default is disable.</td></tr>
<tr><td>0x1102(4354)</td><td>Read</td><td>1word</td><td>Start address of input image word register. =0x0000</td></tr>
<tr><td>0x1103(4355)</td><td>Read</td><td>1word</td><td>Start address of output image word register. =0x0800</td></tr>
<tr><td>0x1104(4356)</td><td>Read</td><td>1word</td><td>Size of input image word register.</td></tr>
<tr><td>0x1105(4357)</td><td>Read</td><td>1word</td><td>Size of output image word register.</td></tr>
<tr><td>0x1106(4358)</td><td>Read</td><td>1word</td><td>Start address of input image bit. = 0x0000</td></tr>
<tr><td>0x1107(4359)</td><td>Read</td><td>1word</td><td>Start address of output image bit. =0x1000</td></tr>
<tr><td>0x1108(4360)</td><td>Read</td><td>1word</td><td>Size of input image bit.</td></tr>
<tr><td>0x1109(4361)</td><td>Read</td><td>1word</td><td>Size of output image bit.</td></tr>
<tr><td>0x110A(4362)</td><td>Read</td><td>1word</td><td>Update time for cyclic data change (same as 0x1028)</td></tr>
<tr><td>0x110E(4366)</td><td>Read</td><td>upto 33word</td><td>Expansion slot’s M-number including
First 1word is adapter’s number, if M9289, then 0x9289</td></tr>
<tr><td>0x1110(4368)</td><td>Read</td><td>1word</td><td>Number of expansion slot</td></tr>
<tr><td>0x1113(4371)</td><td>Read</td><td>upto 33word</td><td>Expansion slot Module Id.
First 1word is adapter’s product code.</td></tr>
<tr><td>0x1119(4377)</td><td>Read</td><td>1word</td><td>Hi byte is ModBus status, low byte is internal status.
Zero value means ‘no error’.
<table>
<tr><th>ModBus Status</th><th>Internal bus status(M-Bus)</th></tr>
<tr><td>0x00 : No Error
0x01 : ERR_DIP_SWITCH
0x40 : ERR_CRC_LRC
0x80 : ERR_WATCHDOG</td><td>0x01 : INIT_STATE
0x02 : IDLE_STATE
0x03 : RUN_STATE
0x04 : STOP_STATE
0x05 : FAULT_STATE
0x06 : RESET_STATE
0x07 : CRCERR_STATE
0x08 : PAUSE_STATE
0x09 : COMM_ERROR_STATE
0x80* : At Hot swap mode expansion module error</td></tr>
</table></td></tr>
<tr><td>0x111D(4381)</td><td>Read</td><td>1word</td><td>Adapter M-Series Revision.</td></tr>
</table>

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

3.4.7. Expansion Slot Information Special Resister (0x2000, 8192)

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

Slot#1 0x2000(8192)~0x201F(8223) Slot#2 0x2020(8224)~0x203F(8255)
Slot#3 0x2040(8256)~0x205F(8287) Slot#4 0x2060(8288)~0x207F(8319)
Slot#5 0x2080(8320)~0x209F(8351) Slot#6 0x20A0(8352)~0x20BF(8383)
Slot#7 0x20C0(8384)~0x20DF(8415) Slot#8 0x20E0(8416)~0x20FF(8447)
Slot#9 0x2100(8448)~0x211F(8479) Slot#10 0x2120(8480)~0x213F(8511)
Slot#11 0x2140(8512)~0x215F(8543) Slot#12 0x2160(8544)~0x217F(8575)
Slot#13 0x2180(8576)~0x219F(8607) Slot#14 0x21A0(8608)~0x21BF(8639)
Slot#15 0x21C0(8640)~0x21DF(8671) Slot#16 0x21E0(8672)~0x21FF(8703)
Slot#17 0x2200(8704)~0x221F(8735) Slot#18 0x2220(8736)~0x223F(8767)
Slot#19 0x2240(8768)~0x225F(8799) Slot#20 0x2260(8800)~0x227F(8831)
Slot#21 0x2280(8832)~0x229F(8863) Slot#22 0x22A0(8864)~0x22BF(8895)
Slot#23 0x22C0(8896)~0x22DF(8927) Slot#24 0x22E0(8928)~0x22FF(8959)
Slot#25 0x2300(8960)~0x231F(8991) Slot#26 0x2320(8992)~0x233F(9023)
Slot#27 0x2340(9024)~0x235F(9055) Slot#28 0x2360(9056)~0x237F(9087)
Slot#29 0x2380(9088)~0x239F(9119) Slot#30 0x23A0(9120)~0x23BF(9151)
Slot#31 0x23C0(9152)~0x23DF(9183) Slot#32 0x23E0(9184)~0x23FF(9215)
Slot#33 0x2400(9216)~0x241F(9247) Slot#34 0x2420(9248)~0x243F(9279)
…..
Slot#63 0x27C0(10176)~0x27DF(10207)

Address Offset	Expansion Slot#1	Expansion Slot#2	Expansion Slot#3	Expansion Slot#4	……..	Expansion Slot#63
+ 0x00(+0)	0x2000(8192)	0x2020(8224)	0x2040(8256)	0x2060(8288)	…….	0x27C0(10176)
+ 0x01(+1)	0x2001(8193)	0x2021(8225)	0x2041(8257)	0x2061(8289)	…….	0x27C1(10177)
+ 0x02(+2)	0x2002(8194)	0x2022(8226)	0x2042(8258)	0x2062(8290)	…….	0x27C2(10178)
+ 0x03(+3)	0x2003(8195)	0x2023(8227)	0x2043(8259)	0x2063(8291)	…….	0x27C3(10179)
+ 0x04(+4)	0x2004(8196)	0x2024(8228)	0x2044(8260)	0x2064(8292)	…….	0x27C4(10180)
+ 0x05(+5)	0x2005(8197)	0x2025(8229)	0x2045(8261)	0x2065(8293)	…….	0x27C5(10181)
+ 0x06(+6)	0x2006(8198)	0x2026(8230)	0x2046(8262)	0x2066(8294)	…….	0x27C6(10182)
+ 0x07(+7)	0x2007(8199)	0x2027(8231)	0x2047(8263)	0x2067(8295)	…….	0x27C7(10183)
+ 0x08(+8)	0x2008(8200)	0x2028(8232)	0x2048(8264)	0x2068(8296)	…….	0x27C8(10184)
+ 0x09(+9)	0x2009(8201)	0x2029(8233)	0x2049(8265)	0x2069(8297)	…….	0x27C9(10185)
+ 0x0A(+10)	0x200A(8202)	0x202A(8234)	0x204A(8266)	0x206A(8298)	…….	0x27CA(10186)
+ 0x0B(+11)	0x200B(8203)	0x202B(8235)	0x204B(8267)	0x206B(8299)	…….	0x27CB(10187)
+ 0x0C(+12)	0x200C(8204)	0x202C(8236)	0x204C(8268)	0x206C(8300)	…….	0x27CC(10188)
+ 0x0D(+13)	0x200D(8205)	0x202D(8237)	0x204D(8269)	0x206D(8301)	…….	0x27CD(10189)
+ 0x0E(+14)	0x200E(8206)	0x202E(8238)	0x204E(8270)	0x206E(8302)	…….	0x27CE(10190)
+ 0x0F(+15)	0x200F(8207)	0x202F(8239)	0x204F(8271)	0x206F(8303)	…….	0x27CF(10191)
+ 0x10(+16)	0x2010(8208)	0x2030(8240)	0x2050(8272)	0x2070(8304)	…….	0x27D0(10192)
+ 0x11(+17)	0x2011(8209)	0x2031(8241)	0x2051(8273)	0x2071(8305)	…….	0x27D1(10193)
+ 0x12(+18)	0x2012(8210)	0x2032(8242)	0x2052(8274)	0x2072(8306)	…….	0x27D2(10194)
+ 0x13(+19)	0x2013(8211)	0x2033(8243)	0x2053(8275)	0x2073(8307)	…….	0x27D3(10195)
+ 0x14(+20)	0x2014(8212)	0x2034(8244)	0x2054(8276)	0x2074(8308)	…….	0x27D4(10196)
+ 0x15(+21)	0x2015(8213)	0x2035(8245)	0x2055(8277)	0x2075(8309)	…….	0x27D5(10197)
+ 0x16(+22)	0x2016(8214)	0x2036(8246)	0x2056(8278)	0x2076(8310)	…….	0x27D6(10198)
+ 0x17(+23)	0x2017(8215)	0x2037(8247)	0x2057(8279)	0x2077(8311)	…….	0x27D7(10199)
+ 0x18(+24)	0x2018(8216)	0x2038(8248)	0x2058(8280)	0x2078(8312)	…….	0x27D8(10200)
+ 0x19(+25)	0x2018(8217)	0x2038(8249)	0x2058(8281)	0x2078(8313)	…….	0x27D9(10201)
+ 0x1A(+26)	0x201A(8218)	0x203A(8250)	0x205A(8282)	0x207A(8314)	…….	0x27DA(10202)
+ 0x1B(+27)	0x201B(8219)	0x203B(8251)	0x205B(8283)	0x207B(8315)	…….	0x27DB(10203)
+ 0x1C(+28)	0x201C(8220)	0x203C(8252)	0x205C(8284)	0x207C(8316)	…….	0x27DC(10204)
+ 0x1D(+29)	0x201D(8221)	0x203D(8253)	0x205D(8285)	0x207D(8317)	…….	0x27DD(10205)
+ 0x1E(+30)	0x201E(8222)	0x203E(8254)	0x205E(8286)	0x207E(8318)	…….	0x27DE(10206)
+ 0x1F(+31)	0x201F(8223)	0x203F(8255)	0x205F(8287)	0x207F(8319)	…….	0x27DF(10207)

Address Offset	Access	Type, Size	Description
+ 0x02(+2) **	Read	1word	Input start register address of input image word this slot.
+ 0x03(+3) **	Read	1word	Input word's bit offset of input image word this slot.
+ 0x04(+4) **	Read	1word	Output start register address of output image word this slot.
+ 0x05(+5) **	Read	1word	Output word's bit offset of output image word this slot.
+ 0x06(+6) **	Read	1word	Input bit start address of input image bit this slot.
+ 0x07(+7) **	Read	1word	Output bit start address of output image bit this slot.
+ 0x08(+8) **	Read	1word	Size of input bit this slot
+ 0x09(+9) **	Read	1word	Size of output bit this slot
+ 0x0A(+10)**	Read	n word	Read input data this slot
+ 0x0B(+11)**	Read/Write	n word	Read/write output data this slot
+ 0x0E(+14)	Read	1word	M-number, if M-1238, returns 0x1238
+ 0x0F(+15)	Read	String upto 72byte	First 1word is length of valid character string. If M12DF, returns "00 23 4D 31 32 44 46 2C 20 31 36 44 49 2C 20 32 34 56 64 63 2C 20 55 6E 69 76 65 72 73 61 6C 20 31 38 " Valid character size = 0x001E =30 characters, "M12DF, 16DI, 24Vdc, Universal 18RTB"
+ 0x10(+16)	Read	1word	Size of configuration parameter byte
+ 0x11(+17)**	Read/Write	n word	Read/write Configuration parameter data, up to 8byte. Refer to A.2 ***
+ 0x17(+23)	Read	2word	Firmware Revision ex) 0x00010010 (Major revision 1/Minor revision 16, Rev 1.016)
+ 0x19(+25)	Read	2word	Firmware release date.

* 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.

3.5. Supported MODBUS Function Codes

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

4. OBJECT MODELS

EtherNet/IP was developed from a very widely implemented standard used for transferring data between two devices in DeviceNet and ControlNet, called the Common Industrial Protocol (CIP). Every CIP node is modeled as a collection of objects. An object provides an abstract representation of a particular component within a device. Anything not described in object form is not visible through the CIP protocol. CIP objects are structured into classes, instances, and attributes.

A class of objects represents the same kind of system component. An object instance is the actual representation of a particular object within a class. Each instance of a class has the same attributes, but it has its own particular set of attribute values.

The objects and their components are addressed by uniform addressing scheme consisting of:

- Media Access Control Identifier (MAC ID), an integer identification value assigned to each node on a CIP network
- Class Identifier (Class ID), an integer identification value assigned to each Object Class accessible from the network
- Instance Identifier (Instance ID), an integer identification value assigned to an Object Instance that identifies it among all instances of the same class.
- Attribute Identifier (Attribute ID), an integer identification value assigned to a class and/or instance attribute.
- Service code, an integer identification value which denotes a particular object instance and/or object class function.

4.1. Supported Objects

■ **Supported Object**

Name of Object	Type	Number of Instances	Class Code
Identity	Required	1	01_{HEX}
Message Router	Required	1	02_{HEX}
Assembly	Required	2	04_{HEX}
Connection Manager	Required	1	06_{HEX}
Port	Required	1	$F4_{HEX}$
TCP/IP Interface	Required	1	$F5_{HEX}$
Ethernet Link	Required	1	$F6_{HEX}$
FnBus Manager	Vendor-specific	1	70_{HEX}
Expansion Slot	Vendor-specific	1~63	71_{HEX}

4.2. Identity Object

Class Code: 01_{HEX}

4.2.1. Common Services

Service Code	Implemented for		Service Name	Value
	Class	Instance		
0x01	Yes	Yes	Get_Attribute_All	
0x05	No	Yes	Reset	0: Reset Only 1: Reset and Factory Default
0x0E	No	Yes	Get_Attribute_Single	

4.2.2. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
0	1	Get	Revision	UINT	0001_{HEX}
	2	Get	Max Instance	UINT	0001_{HEX}
	6	Get	Maximum ID Number Class Attributes	UINT	0000_{HEX}
	7	Get	Maximum ID Number Instance Attributes	UINT	0000_{HEX}

4.2.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	1	Get	Vendor ID	UINT	741_{DEC} (Crevis Co., Ltd)
	2	Get	Device Type	UINT	$0C_{HEX}$ (Communications Adapter)
	3	Get	Product Code	UINT	$A000_{HEX}$ (M9289)
	4	Get	Revision - Major - Minor	Structure of: USINT USINT	 1 ~ 9 1 ~ 255
	5	Get	Status	WORD	Device status. Defined in standard.
	6	Get	Serial Number	UDINT	Unique Number
	7	Get	Product Name - String Length - ASCII String	Short_String USINT STRING	34_{DEC} “M9289,ETHERNET TCP/IP Adapter,MBUS”
	Vendor-specific				
	100	Get	Device Fault Code	USINT	03_{HEX} : Normal Operation See modbus register 0x1119
	104	Get	Firmware Release Date	UDINT	$YYYYMMDD_{HEX}$

4.3. Message Router Object

Class Code: 02_{HEX}

4.3.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x01	Yes	No	Get_Attribute_All
0x0E	No	Yes	Get_Attribute_Single

4.3.2. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
0	1	Get	Revision	UINT	0001_{HEX}
	4	Get	Number of Attribute	UINT	0000_{HEX}
	5		Number of Service	UINT	0000_{HEX}
	6	Get	Maximum ID Number Class Attributes	UINT	0000_{HEX}
	7	Get	Maximum ID Number Instance Attributes	UINT	0000_{HEX}

4.3.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	1	Get	Object Class List	STRUCT of UINT Array of UINT	 10_{DEC} 09 00 01 00 02 00 04 00 06 00 F4 00 F5 00 F6 00 70 00 71 00
	2	Get	Number Available	UINT	16_{DEC} Maximum number of connections supported

4.4. Assembly Object

Class Code: 04 $_{HEX}$

4.4.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x0E	Yes	Yes	Get_Attribute_Single
0x10	No	Yes	Set_Attribute_Single

4.4.2. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
0	1	Get	Revision	UINT	0002_{HEX}

4.4.3. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	3	Get	Input (Produced) Process Image Data	Array n BYTE	Input process image data
2	3	Set/Get	Output (Consumed) Process Image Data	Array n BYTE	Output process image data

4.5. Connection Manager Object

Class Code: 06_{HEX}

4.5.1. Class Attributes, Instance Attribute

None

4.6. Port Object

Class Code: $F4_{HEX}$

4.6.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x01	Yes	Yes	Get_Attribute_All
0x0E	Yes	Yes	Get_Attribute_Single

4.6.2. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
0	1	Get	Revision	UINT	0001_{HEX}
	2	Get	Max Instance	UINT	0001_{HEX}
	3	Get	Num Instances	UINT	0001_{HEX}
	8	Get	Entry Port	UINT	0001_{HEX}
	9	Get	All Ports	ARRAY of STRUCT UINT UINT	0000_{HEX} 0000_{HEX} 0004_{HEX} 0002_{HEX}

4.6.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	1	Get	Port Type	UINT	0004_{HEX} , TCP/IP Port
	2	Get	Port Number	UINT	0002_{HEX}, CIP port number associate with port
	3	Get	Port Object	UINT Padded EPATH	
	4	Get	Port Name	Short_String	=0
	7	Get	Node Address	Padded EPATH	

4.7. TCP/IP Object

Class Code: $F5_{HEX}$

4.7.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x01	Yes	Yes	Get_Attribute_All
0x0E	Yes	Yes	Get_Attribute_Single
0x02	No	Yes	Set_Attribute_All
0x10	No	Yes	Set_Attribute_Single

4.7.2. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
0	1	Get	Revision	UINT	0001_{HEX}
	2	Get	Max Instance	UINT	0001_{HEX}
	3	Get	Num Instances	UINT	

4.7.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	1	Get	Status	DWORD	See section 5.7.3.1.
	2	Get	Configuration Capability	DWORD	00000006_{HEX}
	3	Get/Set	Configuration Control	DWORD	See section 5.7.3.2.
	4	Get	Physical Link Path Size of Path Path	STRUCT of: UINT Padded-PATH	 0002_{HEX} 00 00 20 F6 24 01
	5	Get/Set	Interface Configuration	STRUCT of: UDINT UDINT UDINT UDINT UDINT STRING	 IP address Network Mask Gateway Address Name Server Name Server 2 Domain Name

4.7.3.1. Status Instance Attributes

This attribute indicates the status of the TCP/IP network interface.

Table 4.7.1. Status Attribute

Bit	Description
0-3	0 – The Interface Configuration attribute has not been configured. 1 – The Interface Configuration attribute contains valid configuration from BOOTP, DHCP, or non-volatile storage. 2 – The Interface Configuration attribute contains valid configuration, obtained from DIP switch. 3-15 – Reserved.
4	Indicates pending configuration change in TTL and/or Mcast config.
5-31	Reserved

4.7.3.2. Configuration Control Instance Attributes

This attribute is a bitmap to control network configuration.

Table 4.7.1. Configuration Control Attribute

Bit	Description
0-3	Determine how the device shall obtain its initial configuration at startup. 0 – The device shall use the interface configuration values previously stored in EEPROM. 1 – The device shall use the interface configuration values via BOOTP. 2 – The device shall use the interface configuration values via DHCP upon start-up. 3-15 – Reserved.
4	If TRUE, the device shall resolve host names by querying a DNS server.
5-31	Reserved

4.8. Ethernet Link Object

Class Code: $F6_{HEX}$

4.8.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x01	Yes	Yes	Get_Attribute_All
0x0E	Yes	Yes	Get_Attribute_Single

4.8.2. Class Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
0	1	Get	Revision	UINT	0002_{HEX}
	2	Get	Max Instance	UINT	0001_{HEX}
	3	Get	Num Instances	UINT	0001_{HEX}

4.8.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	1	Get	Interface Speed	UDINT	10_{DEC}, 100_{DEC}
	2	Get	Interface Flags	DWORD	Bit 0 : Link Active Bit 1 : Full Duplex Bit 2~4 : Auto negotiation Bit 5 : Manual Setting required Reset Bit 6 : Local Hardware Fault Others : 0
	3	Get	Physical Address	ARRAY of 6 USINTs	Same as MAC address

4.9. M-Bus Manager Object

Class Code: 70_{HEX}

4.9.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x0E	No	Yes	Get_Attribute_Single
0x10	No	Yes	Set_Attribute_Single

4.9.2. Class Attributes

None

4.9.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1	1	Get	Number of I/O Slot	USINT	(include deactivated slot)
	2	Get	Num of Activated Slot	USINT	
	3	Get	Num of Deactivated Slot	USINT	
	4	Get	External IDs	Array of 64 WORD	See Table 5.9.6.
	5	Get	Selection of Input (Produced) Process Image Mode	USINT	(default 2) Fixed
	6	Get	Selection of Output (Consumed) Process Image Mode	USINT	(default 0) Fixed
	10	Get	Fn-Bus Status	USINT	0x01 : INIT_STATE 0x02 : IDLE_STATE 0x03 : RUN_STATE 0x04 : STOP_STATE 0x05 : FAULT_STATE 0x06 : RESET_STATE 0x07 : CRCERR_STATE 0x08 : PAUSE_STATE
	11	Get	Input (Produced) Byte Size	UINT	IO input byte size
	12	Get	Output (Consumed) Byte Size	UINT	IO output byte size
	13	Get/Set*	Enable Input Run/Idle Header	BOOL	0:Disabled Input Run/Idle Header (default) Fixed
	14	Get/Set*	Enable Output Run/Idle Header	BOOL	1:Enabled Output Run/Idle Header (default) Fixed
	15	Get/Set*	Output Reset at stop	BOOL	0:Disable(default) 1:Enable
	48	Get/Set	Quick Connection	BOOL	0:Disable(default) 1:Enable Port1 : MDI, Port2 : MDIX 100Mbps Fulldupelx only

Table 4.9.6. External IDs (=Expansion Module ID)

Word	Description
0	Network Adapter Module External ID = 0x00
1	External ID for slot position #1
2	External ID for slot position #2
.	.

. .	. .
62	External ID for slot position #62
63	External ID for slot position #63

4.10. Expansion Slot Object

Class Code: 71_{HEX}

4.10.1. Common Services

Service Code	Implemented for		Service Name
	Class	Instance	
0x0E	No	Yes	Get_Attribute_Single
0x10	No	Yes	Set_Attribute_Single

4.10.2. Class Attributes

None

4.10.3. Instance Attributes

Instance ID	Attribute ID	Access Rule	Name	Data Type	Value
1~63 (Slot Address)	1	Get	Module External ID	USINT	Crevis Module ID
	2	Get	I/O Data Code - Input Data Code - Output Data Code	Structure of: USINT USINT	
	3	Get	Input Offset Table - Byte Offset - Bit Offset	Structure of: USINT USINT	Byte offset in the Input Assembly Corresponding bit offset in the byte (If Input data length is zero, then return Empty.)
	4	Get	Output Offset Table - Byte Offset - Bit Offset	Structure of: USINT USINT	Byte offset in the Output Assembly Corresponding bit offset in the byte (If Output data length is zero, then return Empty.)
	5	Get	Input Data	Array of BYTE	Read Input data size defined by attribute 2. If Input data length is zero, then return Empty.
	6	Get/Set	Output Data	Array of BYTE	Read/Write Output data size defined by attribute 2. If Output data length is zero, then return Empty.
	7	Get/	Active Flag	BOOL	0: This slot is activated 1: This slot is deactivated
	8	Get	Configuration Parameter Data length	USINT	FnBUS I/O Parameter
	100	Get	Product Code	4 Byte	
	101	Get	Catalog Number	4 Byte	
	102	Get	Firmware Revision	Structure of: USINT USINT	Expansion Module Firmware Revision

4.11. Ethernet/IP Reference

Ethernet/IP Reference Documents
http://www.odva.org
http://www.ethernet-ip.org
Ethernet/IP Tools
http://www.pyramid-solutions.com