
FnIO G - Series:

GN-9287

GN-9287 (Profinet Network Adapter)

Table of Contents

1.Environment Specification.....	5
2.GN-9287 (PROFINET NETWORK ADAPTER).....	6
2.1 GN-9287 Specification.....	6
2.2 GN-9287 Wiring Diagram.....	7
2.3 GN-9287 LED Indicator.....	8
2.3.1 LED Indicator.....	8
2.3.2 MOD (Module Status LED).....	8
2.3.3 NET (Network Status LED).....	8
2.3.4 ERROR (Error Status LED).....	8
2.3.5 IOS LED (Extension Module Status LED).....	8
2.3.6 Field Power, System Power LED (Field Power, System Power Status LED).....	8
2.4 GN-9287 Electrical Interface.....	9
2.4.1 RJ-45 Socket.....	9
2.4.2 Dip Switch.....	9
2.4.3 RS232 Port for MODBUS/RTU, Touch Pannel.....	10
3.I/O Process Image Map.....	11
3.1 Mapping Data into Image Table.....	11
3.1.1 Discrete Input Module.....	11
3.1.2 Discrete Output Module.....	12
3.1.3 Analog Input Module.....	13
3.1.4 Analog Output Module.....	14
3.2 Example of Input Process Image (Input Register) Map.....	15
3.3 Example of Output Process Image (Output Register) Map.....	16
4.PARAMETER.....	17
4.1 GN-9287 Parameter.....	17
4.2 GN-9287 PROFINET IO Characteristics.....	17
4.2.1 Device Identity.....	17
4.2.2 Device Access Point.....	17
4.2.3 Sub-slot of GN-9287.....	18
5.MODBUS Interface.....	19
5.1 MODBUS Interface Register/Bit Map.....	19
5.2 Surppoorted MODBUS Function Codes.....	19
5.2.1 8 (0x08) Diagnostics.....	21
5.2.2 Error Response.....	22
5.3 MODBUS Special Register Map.....	23

5.3.1 Adapter Identification Special Register (0x1000, 4096).....	23
5.3.2 Other Time Special Register (0x1028, 4136).....	23
5.3.3 Adapter IP/MAC Address Special Register (0x1050, 4176).....	23
5.3.4 Adapter Information Special Register (0x1100, 4352).....	24
5.3.5 Expansion Slot Information Special Resister (0x2000, 8192).....	25
5.4 MODBUS Reference.....	26

History

Rev	Pages	Remarks	Date	Editor
1.00			August 30, 2018	Joonho, Park
-		Update	January 15, 2019	Joonho, Park
-		NET LED / ERROR LED Indicator Update	February 14, 2019	Joonho, Park
-		GN-9287 Parameter Update	February 20, 2019	Joonho, Park
-		Adapter Identification Special Register Update	April 03, 2019	Joonho, Park
-		Adapter Information Special Register Update	April 09, 2019	Joonho, Park
1.01		IAP Mode Setting Update	October 10, 2019	Joonho, Park
1.02		NA Parameter Data Update	March 03, 2020	Joonho, Park
1.03		Revision related to UL certification	March 10, 2020	GWLEE
1.03	20	Modbus special register map Update(0x1119)	July 07, 2020	Joonho, Park
1.04	11	DIP Switch Function Update	March 26, 2021	Joonho, Park
1.05	10	Changed system/field power LED indicate	June 01, 2023	Joonho, Park
1.06	All		Aug. 24, 2023	Joonho, Park
1.07	8	Error Slot LED Indication Added	Aug. 22, 2025	Seonghyeon, Park

1. Environment Specification

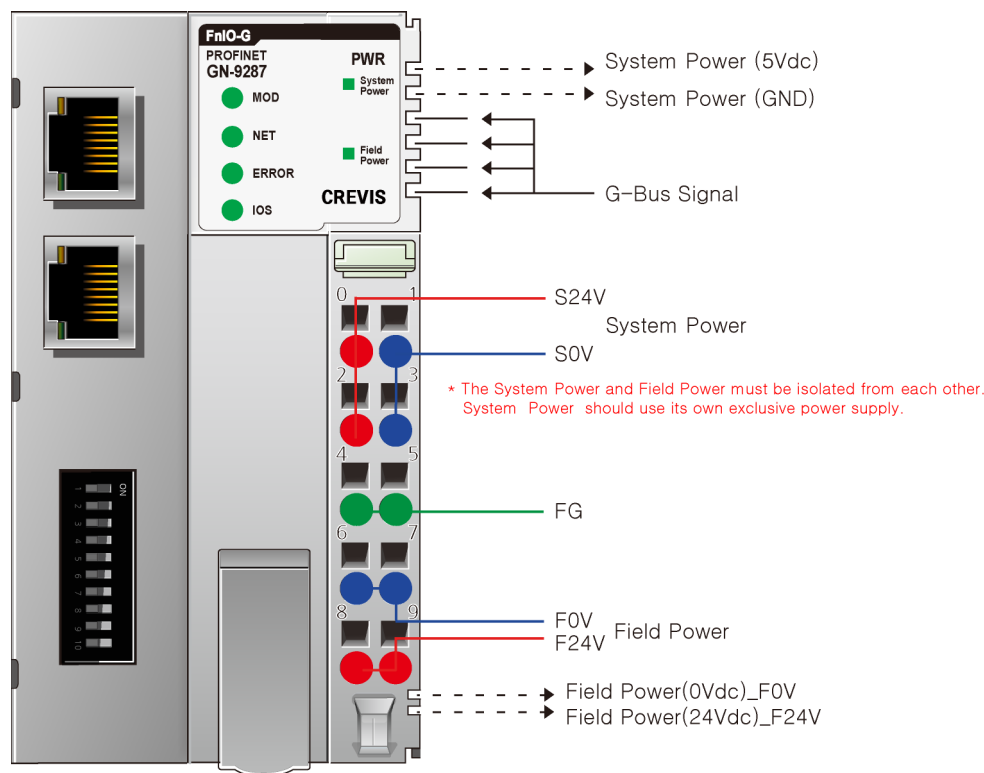
Environmental specification	
Operating Temperature	-40°C ~ 60°C : 1.5A full load is allowed.
UL Temperature	-20°C ~ 60°C
Storage Temperature	-40°C ~ 85°C
Relative Humidity	5% ~ 90% non-condensing
Mounting	DIN rail
General specification	
Shock Operating	IEC 60068-2-27
Vibration Resistance	Based on IEC 60068-2-6, 4g
Industrial Emissions	EN 61000-6-4/A11 : 2011
Industrial Immunity	EN 61000-6-2 : 2005
Installation Position	Vertical and horizontal installation is available.
Product Certifications	CE, UL

2. GN-9287 (PROFINET NETWORK ADAPTER)

2.1 GN-9287 Specification

Items	Specification
Communication Specification	
Adapter Type	Slave node (Profinet)
Protocol	Profinet, Modbus RTU
Max. Expansion Module	32 slots
Max. Data Size	Max 1440 bytes
Max Length Bus Line	Up to 100m from Ethernet Hub/Switch with twisted CAT5 UTP/STP
Max. Nodes	Limited by Profinet Specification.
Baud Rate	100Mbps, Auto-negotiation, Full duplex
Interface Connector	RJ-45 socket * 2pcs
IP-Address Setup	Via Master Device Software
Max. Parameter Size	2048 Bytes (ex : 1 slot = 64 Byte + I/O Parameter Size(Dword size))
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
Serial Configuration (RS232)	Node : 1 (Fixed) Baud Rate : 115200 (Fixed) Data bit : 8 (Fixed) Parity bit : No parity (Fixed) Stop bit : 1 (Fixed)
Indicator	6 LED 1 Green/Red, Module Status (MOD) 1 Green, Network Status (NET) 1 Green/Red, Error Status (ERROR) 1 Green/Red, Expansion Module Status (IOS) 1 Green, System Power Status 1 Green, Field Power Status 2 LED (each RJ45 Connector) 1 Yellow, Link/Active 1 Green, Not used
Module Location	Starter module left side of G-Series system
Field Power Detection	About 14Vdc
General specification	
UL System Power	Supply voltage : 24Vdc nominal, Class 2
System Power	Supply voltage : 24Vdc nominal Supply voltage range : 15~30Vdc Protection : Output current limit (Min. 1.5A) Reverse polarity protection
Power Dissipation	70mA typical @ 24Vdc
Current for I/O Module	1.5A @ 5Vdc
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. 30Vdc) * Field Power Range is different depending on IO Module series. Refer to IO Module's Specification.
Max. Current Field Power Contact	DC 10A Max
Wiring	I/O Cable Max. 2.0mm ² (AWG 14)
Weight	172g
Module Size	54mm x 99mm x 70mm
Environment Condition	Refer to '1. Environment Specification'

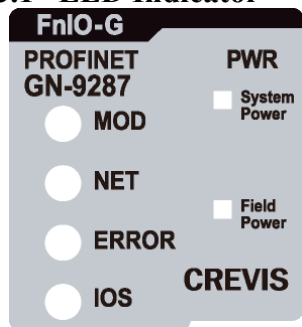
2.2 GN-9287 Wiring Diagram



Pin No.	Signal Description	Signal Description	Pin No.
0	System Power, 24V	System Power, Ground	1
2	System Power, 24V	System Power, Ground	3
4	F.G	F.G	5
6	Field Power, Ground	Field Power, Ground	7
8	Field Power, 24V	Field Power, 24V	9

2.3 GN-9287 LED Indicator

2.3.1 LED Indicator



LED No.	LED Function / Description	LED Color
MOD	Module Status	Green/Red
NET	Network Status	Green/Red
ERROR	Error Status	Red
IOS	Extension Module Status	Green/Red
System Power	System Power Status	Green
Field Power	Field Power Status	Green

2.3.2 MOD (Module Status LED)

Status	LED	To indicate
No Powered	OFF	No power is supplied to the unit.
Device Operational	Green	The unit is operating in normal condition.
Error Slot Indication*	Flashing Green (N times)	Flashing Green led in N times (N = faulty IO position). For 5 seconds the led will be off then this process repeats.
Unrecoverable Fault	Red	The device has an unrecoverable fault. - Memory error or CPU watchdog error.

* During normal operation, only one slot where an error initially occurred is detected.

2.3.3 NET (Network Status LED)

Status	LED	To indicate
No Powered	OFF	No power is supplied to the unit.
Communication	Green	Normal communication.
Communication Ready	Flashing Green	Communication identification.
Invalid Configuration	Flashing Red	DCP Communication error(Invalid Configuration).

2.3.4 ERROR (Error Status LED)

Status	LED	To indicate
No Error	OFF	No Error.
Connection error	Red	Communication connection error.

2.3.5 IOS LED (Extension Module Status LED)

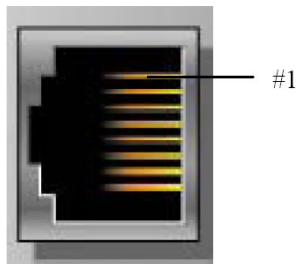
Status	LED	To indicate
Not Powered	OFF	Device may not be powered.
No Expansion Module	Flashing Red	Adapter has no expansion module
Internal Bus Connection, Run Exchanging I/O	Green	Exchanging I/O data.
Expansion Configuration Failed	Red	One or more expansion module occurred in fault state. - Detected invalid expansion module ID. - Overflowed Input/Output Size - Too many expansion module - Initialization failure - Communication failure. - Changed expansion module configuration. - Mismatch vendor code between adapter and expansion module.

2.3.6 Field Power, System Power LED (Field Power, System Power Status LED)

Status	LED	To indicate
Not supplied field, system power	OFF	Not supplied 24Vdc field power, 5Vdc system power.
Supplied field, system power	Green	Supplied 24Vdc field power, 5Vdc system power.

2.4 GN-9287 Electrical Interface

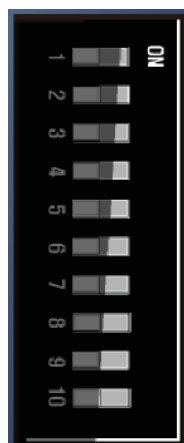
2.4.1 RJ-45 Socket



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 Dip Switch



DIP Pole#	Description	
1	Node ID Bit0	Device Name (GN9287-XX) - XX must a value between 1~99.
2	Node ID Bit1	
3	Node ID Bit2	
4	Node ID Bit3	
5	Node ID Bit4	
6	Node ID Bit5	
7	Node ID Bit6	
8	Reserve	
9	IP Address (By Master)	
10	Node ID : Flash Memory Value	

• **When the dip switch is not set to non-zero (1~99):**

If the decimal value of the dip switch is not zero (0), the name of device will be fixed as “GN9287-xx” (xx: 1~99). You must put the fixed device name.

• **When the dip switch “9 pole” is set to switch ON:**

When the GN-9287 device is powered on, the IP Address, Gateway, and Subnet mask values stored in the EEPROM are set as default values.(Regardless of the dip switch value).

If the IP address, Gateway and Subnet mask values assigned from the master device are different from the stored EEPROM values, The value that assigned from the master are written to the EEPROM.

• **When the dip switch “10 pole” is set to switch ON:**

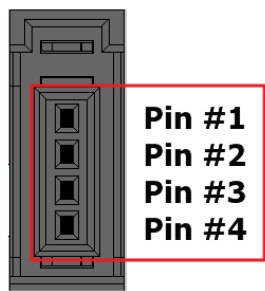
GN-9287 Devices on a PROFINET subnet must have unique names. The device names must satisfy DNS naming conventions. This means that the following rules must be observed:

- Names are limited to a total of 127 characters (letters, numbers, dashes or dots)
- Any component part (that is, a character string between two dots) of the device name may only be up to 63 characters long.
- Names cannot contain any special characters such as umlauts, parentheses, underscores, forward or backward slashes, empty spaces, etc. The dash is the only special character allowed.
- Names must not begin or end with the "-" or "." characters.
- Names must not have the format n.n.n.n (where n = 0...999).
- The device name must not start with numbers.

Device names are assigned to PROFINET IO device when the device is being set up and placed in operation for the first time ("commissioned").

The default name is “GN9287-address”.

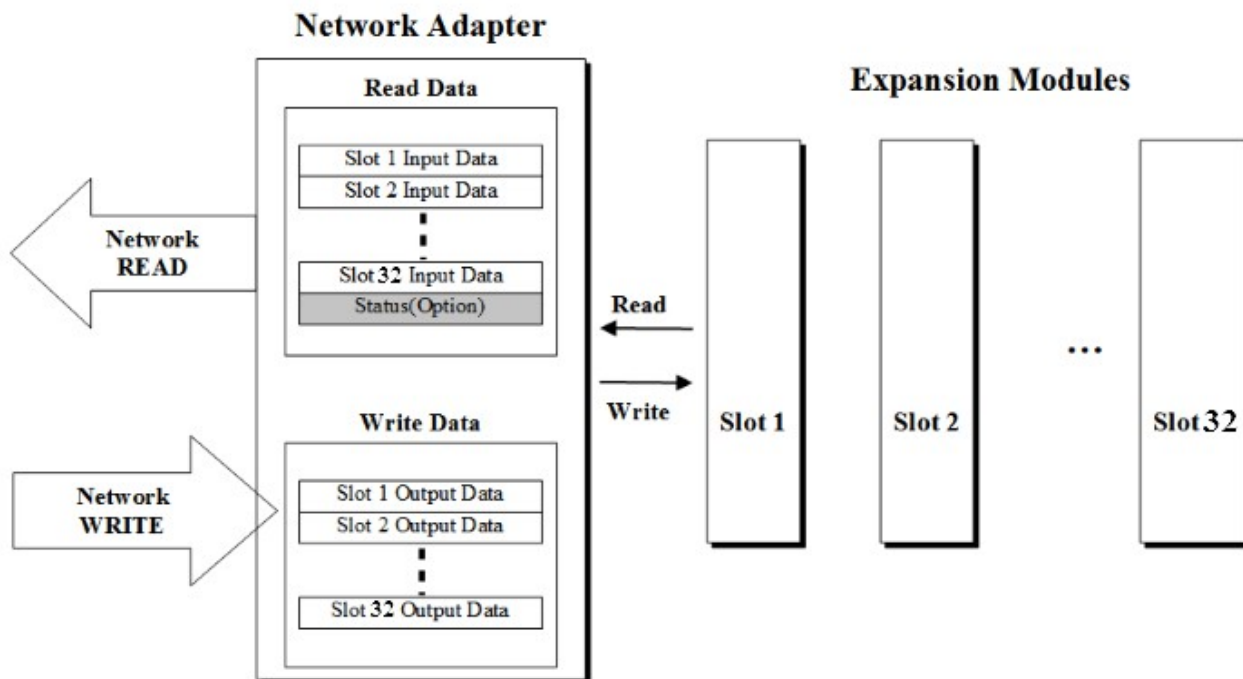
2.4.3 RS232 Port for MODBUS/RTU, Touch Pannel



RS232 (37204-62A3-004PL/3M)		
Pin#	Signal Name	Description
1	Reserved	----
2	TXD	RS232 TXD
3	RXD	RS232 RXD
4	GND	RS232 GND

3. I/O Process Image Map

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



3.1 Mapping Data into Image Table

3.1.1 Discrete Input Module

- 4 Point Input Module

Input Module Data

D3	D2	D1	D0
----	----	----	----



Input Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	Reserved				D3	D2	D1	D0

- 8 Point Input Module

Input Module Data

D7	D6	D5	D4	D3	D2	D1	D0
----	----	----	----	----	----	----	----



Input Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	D7	D6	D5	D4	D3	D2	D1	D0

- 16 Point Input Module

Input Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	D7	D6	D5	D4	D3	D2	D1	D0

Input Module Data

D7	D6	D5	D4	D3	D2	D1	D0
D15	D14	D13	D12	D11	D10	D9	D8

- 32 Point Input Module

Input Module Data

D7	D6	D5	D4	D3	D2	D1	D0
D15	D14	D13	D12	D11	D10	D9	D8
D23	D22	D21	D20	D19	D18	D17	D16
D31	D30	D29	D28	D27	D26	D25	D24



Input Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	D7	D6	D5	D4	D3	D2	D1	D0
Byte 1	D15	D14	D13	D12	D11	D10	D9	D8
Byte 2	D23	D22	D21	D20	D19	D18	D17	D16
Byte 3	D31	D30	D29	D28	D27	D26	D25	D24

3.1.2 Discrete Output Module

- 4 Point Output Module

Output Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	Reserved				D3	D2	D1	D0



Output Module Data

D3	D2	D1	D0
----	----	----	----

- 8 Point Output Module

Output Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	D7	D6	D5	D4	D3	D2	D1	D0



Output Module Data

D7	D6	D5	D4	D3	D2	D1	D0
----	----	----	----	----	----	----	----

- 16 Point Output Module

Output Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	D7	D6	D5	D4	D3	D2	D1	D0
Byte 1	D15	D14	D13	D12	D11	D10	D9	D8



Output Module Data

D7	D6	D5	D4	D3	D2	D1	D0
D15	D14	D13	D12	D11	D10	D9	D8

- 32 Point Output Module

Output Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	D7	D6	D5	D4	D3	D2	D1	D0
Byte 1	D15	D14	D13	D12	D11	D10	D9	D8
Byte 2	D23	D22	D21	D20	D19	D18	D17	D16
Byte 3	D31	D30	D29	D28	D27	D26	D25	D24



Output Module Data

D7	D6	D5	D4	D3	D2	D1	D0
D15	D14	D13	D12	D11	D10	D9	D8
D23	D22	D21	D20	D19	D18	D17	D16
D31	D30	D29	D28	D27	D26	D25	D24

3.1.3 Analog Input Module

- 4 Channel Analog Input Module

Input Module Data

Analog Input Ch0
Analog Input Ch1
Analog Input Ch2
Analog Input Ch3



Input Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	Analog Input Ch0 low byte							
Byte 1	Analog Input Ch0 high byte							
Byte 2	Analog Input Ch1 low byte							
Byte 3	Analog Input Ch1 high byte							
Byte 4	Analog Input Ch2 low byte							
Byte 5	Analog Input Ch2 high byte							
Byte 6	Analog Input Ch3 low byte							
Byte 7	Analog Input Ch3 high byte							

- 8 Channel Analog Input Module

Input Module Data

Analog Input Ch0
Analog Input Ch1
Analog Input Ch2
Analog Input Ch3
Analog Input Ch4
Analog Input Ch5
Analog Input Ch6
Analog Input Ch7



Input Image Value

Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	Analog Input Ch0 low byte							
Byte 1	Analog Input Ch0 high byte							
Byte 2	Analog Input Ch1 low byte							
Byte 3	Analog Input Ch1 high byte							
Byte 4	Analog Input Ch2 low byte							
Byte 5	Analog Input Ch2 high byte							
Byte 6	Analog Input Ch3 low byte							
Byte 7	Analog Input Ch3 high byte							
Byte 8	Analog Input Ch4 low byte							
Byte 9	Analog Input Ch4 high byte							
Byte 10	Analog Input Ch5 low byte							
Byte 11	Analog Input Ch5 high byte							
Byte 12	Analog Input Ch6 low byte							
Byte 13	Analog Input Ch6 high byte							
Byte 14	Analog Input Ch7 low byte							
Byte 15	Analog Input Ch7 high byte							

3.1.4 Analog Output Module

- 4 Channel Analog Input Module

Output Image Value	Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	Analog Output Ch0 low byte								
Byte 1	Analog Output Ch0 high byte								
Byte 2	Analog Output Ch1 low byte								
Byte 3	Analog Output Ch1 high byte								
Byte 4	Analog Output Ch2 low byte								
Byte 5	Analog Output Ch2 high byte								
Byte 6	Analog Output Ch3 low byte								
Byte 7	Analog Output Ch3 high byte								



Output Module Data	Analog Output Ch0
	Analog Output Ch1
	Analog Output Ch2
	Analog Output Ch3

- 8 Channel Analog Input Module

Output Image Value	Bit No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Byte 0	Analog Output Ch0 low byte								
Byte 1	Analog Output Ch0 high byte								
Byte 2	Analog Output Ch1 low byte								
Byte 3	Analog Output Ch1 high byte								
Byte 4	Analog Output Ch2 low byte								
Byte 5	Analog Output Ch2 high byte								
Byte 6	Analog Output Ch3 low byte								
Byte 7	Analog Output Ch3 high byte								
Byte 8	Analog Output Ch4 low byte								
Byte 9	Analog Output Ch4 high byte								
Byte 10	Analog Output Ch5 low byte								
Byte 11	Analog Output Ch5 high byte								
Byte 12	Analog Output Ch6 low byte								
Byte 13	Analog Output Ch6 high byte								
Byte 14	Analog Output Ch7 low byte								
Byte 15	Analog Output Ch7 high byte								



Output Module Data	Analog Output Ch0
	Analog Output Ch1
	Analog Output Ch2
	Analog Output Ch3
	Analog Output Ch4
	Analog Output Ch5
	Analog Output Ch6
	Analog Output Ch7

3.2 Example of Input Process Image (Input Register) Map

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

- For example slot configuration

Slot Address	Module Description
#0	ProfiNet Adapter
#1	8-discrete input
#2	16-discrete input
#3	8-discrete input
#4	16-discrete input
#5	4-analog input
#6	4-analog input

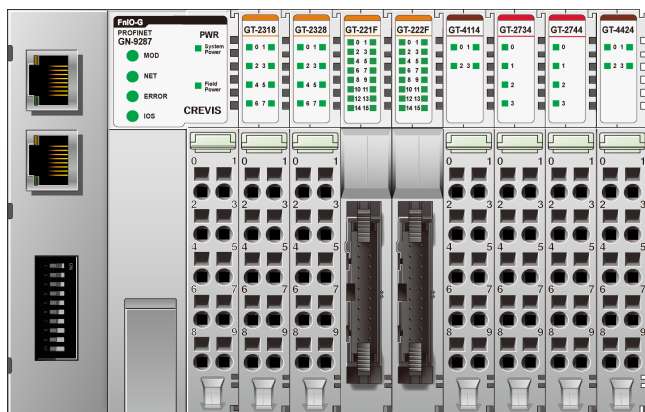
- Input Process Image

Byte	Slot #	Bit 7	Bit 6	Bit5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Read Byte 0	Slot 1	Discrete Input 8 Point							
Read Byte 1	Slot 2	Discrete Input 16 Point low byte							
Read Byte 2		Discrete Input 16 Point high byte							
Read Byte 3	Slot 3	Discrete Input 8 Point							
Read Byte 4	Slot 4	Discrete Input 16 Point low byte							
Read Byte 5		Discrete Input 16 Point high byte							
Read Byte 6	Slot 5	Analog Input Ch0 low byte							
Read Byte 7		Analog Input Ch0 high byte							
Read Byte 8		Analog Input Ch1 low byte							
Read Byte 9		Analog Input Ch1 high byte							
Read Byte 10		Analog Input Ch2 low byte							
Read Byte 11		Analog Input Ch2 high byte							
Read Byte 12		Analog Input Ch3 low byte							
Read Byte 13		Analog Input Ch3 high byte							
Read Byte 14	Slot 6	Analog Input Ch0 low byte							
Read Byte 15		Analog Input Ch0 high byte							
Read Byte 16		Analog Input Ch1 low byte							
Read Byte 17		Analog Input Ch1 high byte							
Read Byte 18		Analog Input Ch2 low byte							
Read Byte 19		Analog Input Ch2 high byte							
Read Byte 20		Analog Input Ch3 low byte							
Read Byte 21		Analog Input Ch3 high byte							

3.3 Example of Output Process Image (Output Register) Map

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

- For example slot configuration



Slot Address	Module Description
#0	ProfiNet Adapter
#1	8-discrete output
#2	8-discrete output
#3	16-discrete output
#4	16-discrete output
#5	4-analog output
#6	4-relay output
#7	4-relay output
#8	4-analog output

- Output Process Image

Byte	Slot #	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Write Byte 0	Slot 1	Discrete Output 8 Point							
Write Byte 1	Slot 2	Discrete Output 8 Point							
Write Byte 2	Slot 3	Discrete Output 16 Point low byte							
Write Byte 3		Discrete Output 16 Point high byte							
Write Byte 4	Slot 4	Discrete Output 16 Point low byte							
Write Byte 5		Discrete Output 16 Point high byte							
Write Byte 6	Slot 5	Analog Output Ch0 low byte							
Write Byte 7		Analog Output Ch0 high byte							
Write Byte 8		Analog Output Ch1 low byte							
Write Byte 9		Analog Output Ch1 high byte							
Write Byte 10		Analog Output Ch2 low byte							
Write Byte 11		Analog Output Ch2 high byte							
Write Byte 12		Analog Output Ch3 low byte							
Write Byte 13		Analog Output Ch3 high byte							
Write Byte 14	Slot 6	Not used				Discrete Output 4 Point			
Write Byte 15	Slot 7	Not used				Discrete Output 4 Point			
Write Byte 16	Slot 8	Analog Output Ch0 low byte							
Write Byte 17		Analog Output Ch0 high byte							
Write Byte 18		Analog Output Ch1 low byte							
Write Byte 19		Analog Output Ch1 high byte							
Write Byte 20		Analog Output Ch2 low byte							
Write Byte 21		Analog Output Ch2 high byte							
Write Byte 22		Analog Output Ch3 low byte							
Write Byte 23		Analog Output Ch3 high byte							

4. PARAMETER

4.1 GN-9287 Parameter

Parameter	Setting	Description
Word data type	All type	Little Endian format(LSB-MSB)
Stop action	Clear output image to 0 *	All outputs are set to 0.
	Hold last valid output image	All outputs are remain the last value.
Stop action_Mode	General Mode *	For SIEMENS PLC
	Special Mode	For Soft PLC(ex-CoDeSys)

* : Default setting

4.2 GN-9287 PROFINET IO Characteristics

4.2.1 Device Identity

Item	Value
Vendor	CREVIS
Vendor ID	0x0140
Product family	CREVIS FnIO System
Device ID	0x9A00
Details	GN9287 PROFINET IO Device

4.2.2 Device Access Point

Item	Value
Module Ident Number	0x00009A00
Details	GN9287 PROFINET IO Device
Vendor Name	CREVIS
Order Number	GN-9287
Category	CREVIS PROFINET I/O
Software Version	V1.0
Hardware Version	V1.0
Maximal Input Length	1440 Bytes
Maximal Output Length	1440 Bytes
Physical Slots	0..32
Minimal Device Interval	4msec
Based on	portStack
DNS Compliant Name	GN9287-xx
Supports Extended Assignment of IP Address	No
Fixed in Slots	0
Instance Field of the Object UUID	1
Supports Multiple Write	Yes
Requires IOPS/IOCS	Yes
Requires Engineering tool which supports at least GSDML Version	V2.32

4.2.3 Sub-slot of GN-9287

Item	Value
Sub-slot Number	Sub-slot Label
32768 (0x8000)	X1
32769 (0x8001)	P1

Sub-module	
Sub-module Ident Number	0x00000001

GN-9287 Parameters (Index : 1, Length : 2Bytes, Transfer sequence : 0)								
Byte Offset	Data							
0	0x00, 0x00							
Name of Parameter	Data Type	Byte Offset	Bit Offset	Bit Length	Default value	Value Range	Changeable	Visible
Word data format	Bit Area	0	0	1	MOTOROLA	0..1	Yes	Yes
Stop action	Bit Area	1	0	1	Clear output images to 0	0..1	Yes	Yes

Interface : GN-9287	
Sub-module Ident Number	0x0002
Sub-slot Number	32768 (0x8000)
Supports Real time Class	Class 1
Supports Isochronous Mode	No
Number of Additional Input CRs	0
Number of Additional Output CRs	0
Number of Additional Multicast Provider CRs	0
Number of Multicast Consumer CRs	0
Supported Send-clock Factors (Base 31.25us)	32 64 128
Supported Reduction Ratios	1 2 4 8 16 32 64 128 256 512

Port 1 : Port 1	
Sub-module Ident Number	0x0003
Sub-slot Number	32769 (0x8001)
MAU Type	100BASETXFD

5. MODBUS Interface

5.1 MODBUS Interface Register/Bit Map

- Register Map

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

- Register Map

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

5.2 Supported MODBUS Function Codes

Function Code	Function	Description
1(0x01)	Read Coils (Read output bit)	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.
2(0x02)	Read Discrete Inputs (Read input bit)	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.
3(0x03)	Read Holding Registers (Read output word)	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.

4(0x04)	Read Input Registers (Read input word)	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.
5(0x05)	Write Single Coil (Write one bit output)	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.
6(0x06)	Write Single Register (Write one word output)	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.
8(0x08)	Diagnostics (Read diagnostic register) *Refer to the 4.2.1	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.
15(0x0F)	Write Multiple Coils (Write a number of output bits)	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.
16(0x10)	Write Multiple registers (Write a number of output words)	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.
23(0x17)	Read/Write Multiple registers (Read a number of input words /Write a number of output words)	Read a number of input words /Write a number of output words 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.

– Refer to MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1a

5.2.1 8 (0x08) Diagnostics

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, 0xFF00	Echo Request Data	Reset Only

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 Module Status

The response data field returns the status of ModBus and expansion module addressed to the remote device.
This status values are identical with status 1 word of input process image. Refer to 2.4.2.

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

5.2.2 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 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.

5.3 MODBUS Special Register Map

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

5.3.1 Adapter Identification Special Register (0x1000, 4096)

Address	Access	Type, Size	Description
0x1000(4096)	Read	1word	Vendor ID = 0x0140(320), Crevis. Co., Ltd.
0x1001(4097)	Read	1word	Device type = 0x000C, Network Adapter
0x1002(4098)	Read	1word	Product Code = 0x9070
0x1003(4099)	Read	1word	Firmware revision, if 0x0101, revision 1.01
0x1004(4100)	Read	2words	Product unique serial number
0x1005(4101)	Read	String upto 34bytes	Product name string (ASCII) “GN-9287,PROFINET,GBUS”
0x1006(4102)	Read	1word	Sum check of EEPROM
0x1010(4112)	Read	2words	Firmware release date
0x1011(4113)	Read	2words	Product manufacturing inspection date
0x101E(4126)	Read	7words - 1word - 1word - 1word - 1word - 1word - 2words	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

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

5.3.2 Other Time Special Register (0x1028, 4136)

Address	Access	Type, Size	Description
0x1028(4136)	Read	1word	IO update time, main loop time. (1usec unit)

5.3.3 Adapter IP/MAC Address Special Register (0x1050, 4176)

Address	Access	Type, Size	Description
0x1050(4176)	Read/ Write	2words	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	2words	Subnet mask. If 255.255.255.0, then 0xFFFF, 0x00FF.
0x1052(4178)	Read/ Write	2words	Gateway. If 192.168.123.254, then 0xA8C0, 0xFE7B.
0x1053(4179)	Read	3words	Ethernet physical address (MAC-ID). If 11-22-33-44-55-66, then 0x2211, 0x4433, 0x6655.

5.3.4 Adapter Information Special Register (0x1100, 4352)

Address	Access	Type, Size	Description				
0x1100(4352)*	Read	1word	Current STATION-NUMBER. If Dip SW 10 = Off				
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.				
0x110A(4362)	Read	1word	Update time for cyclic data change (same as 0x1028)				
0x110D(4365)	Read	1word	Current Dip Switch State and Field Power Status (MSB) ex) Flash memory Value using, Dip SW(0x01), Field Power On = 0x8201				
0x110E(4366)	Read	upto 33words	Expansion slot's GT-number including GN First 1word is adapter's number, if GN-9287, then 0x9287				
0x1110(4368)	Read	1word	Number of expansion slot				
0x1113(4371)	Read	upto 33words	Expansion slot Module Id. First 1word is adapter's module id.				
0x1119(4377)	Read	1word	Hi byte is ModBus status, low byte is internal bus status. Zero value means 'no error'.				
			<table><tr><th>ModBus status</th><th>Internal bus status(G-Bus)</th></tr><tr><td></td><td>0x00 : OPERATING 0x01 : COMMUNICATION_FAULT 0x02 : CONNECT_FAULT 0x03 : CONFIG_FAULT 0x04 : NO_EXPANSION 0x05 : NVALID_ATTR_VALUE 0x06 : TOO_MUCH_DATA 0x07 : VENDOR_ERROR 0x08 : NOT_EXPECTED_SLOT 0x09 : CRC_ERROR 0x80 : NO FIELD POWER</td></tr></table>	ModBus status	Internal bus status(G-Bus)		0x00 : OPERATING 0x01 : COMMUNICATION_FAULT 0x02 : CONNECT_FAULT 0x03 : CONFIG_FAULT 0x04 : NO_EXPANSION 0x05 : NVALID_ATTR_VALUE 0x06 : TOO_MUCH_DATA 0x07 : VENDOR_ERROR 0x08 : NOT_EXPECTED_SLOT 0x09 : CRC_ERROR 0x80 : NO FIELD POWER
			ModBus status	Internal bus status(G-Bus)			
	0x00 : OPERATING 0x01 : COMMUNICATION_FAULT 0x02 : CONNECT_FAULT 0x03 : CONFIG_FAULT 0x04 : NO_EXPANSION 0x05 : NVALID_ATTR_VALUE 0x06 : TOO_MUCH_DATA 0x07 : VENDOR_ERROR 0x08 : NOT_EXPECTED_SLOT 0x09 : CRC_ERROR 0x80 : NO FIELD POWER						
0x111D(4381)	Read	1word	Adapter G-Series Revision.				

* 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).

5.3.5 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#32 0x23E0(9184)~0x23FF(9215)

Address Offset	Expansion Slot#1	Expansion Slot#2	Expansion Slot#3	Expansion Slot#32
+ 0x00(+0)	0x2000(8192)	0x2020(8224)	0x2040(8256)	0x27C0(10176)
+ 0x01(+1)	0x2001(8193)	0x2021(8225)	0x2041(8257)	0x27C1(10177)
+ 0x02(+2)	0x2002(8194)	0x2022(8226)	0x2042(8258)	0x27C2(10178)
+ 0x03(+3)	0x2003(8195)	0x2023(8227)	0x2043(8259)	0x27C3(10179)
+ 0x04(+4)	0x2004(8196)	0x2024(8228)	0x2044(8260)	0x27C4(10180)
+ 0x05(+5)	0x2005(8197)	0x2025(8229)	0x2045(8261)	0x27C5(10181)
+ 0x06(+6)	0x2006(8198)	0x2026(8230)	0x2046(8262)	0x27C6(10182)
+ 0x07(+7)	0x2007(8199)	0x2027(8231)	0x2047(8263)	0x27C7(10183)
+ 0x08(+8)	0x2008(8200)	0x2028(8232)	0x2048(8264)	0x27C8(10184)
+ 0x09(+9)	0x2009(8201)	0x2029(8233)	0x2049(8265)	0x27C9(10185)
+ 0x0A(+10)	0x200A(8202)	0x202A(8234)	0x204A(8266)	0x27CA(10186)
+ 0x0B(+11)	0x200B(8203)	0x202B(8235)	0x204B(8267)	0x27CB(10187)
+ 0x0C(+12)	0x200C(8204)	0x202C(8236)	0x204C(8268)	0x27CC(10188)
+ 0x0D(+13)	0x200D(8205)	0x202D(8237)	0x204D(8269)	0x27CD(10189)
+ 0x0E(+14)	0x200E(8206)	0x202E(8238)	0x204E(8270)	0x27CE(10190)
+ 0x0F(+15)	0x200F(8207)	0x202F(8239)	0x204F(8271)	0x27CF(10191)
+ 0x10(+16)	0x2010(8208)	0x2030(8240)	0x2050(8272)	0x27D0(10192)
+ 0x11(+17)	0x2011(8209)	0x2031(8241)	0x2051(8273)	0x27D1(10193)
+ 0x12(+18)	0x2012(8210)	0x2032(8242)	0x2052(8274)	0x27D2(10194)
+ 0x13(+19)	0x2013(8211)	0x2033(8243)	0x2053(8275)	0x27D3(10195)
+ 0x14(+20)	0x2014(8212)	0x2034(8244)	0x2054(8276)	0x27D4(10196)
+ 0x15(+21)	0x2015(8213)	0x2035(8245)	0x2055(8277)	0x27D5(10197)
+ 0x16(+22)	0x2016(8214)	0x2036(8246)	0x2056(8278)	0x27D6(10198)
+ 0x17(+23)	0x2017(8215)	0x2037(8247)	0x2057(8279)	0x27D7(10199)
+ 0x18(+24)	0x2018(8216)	0x2038(8248)	0x2058(8280)	0x27D8(10200)
+ 0x19(+25)	0x2018(8217)	0x2038(8249)	0x2058(8281)	0x27D9(10201)
+ 0x1A(+26)	0x201A(8218)	0x203A(8250)	0x205A(8282)	0x27DA(10202)
+ 0x1B(+27)	0x201B(8219)	0x203B(8251)	0x205B(8283)	0x27DB(10203)
+ 0x1C(+28)	0x201C(8220)	0x203C(8252)	0x205C(8284)	0x27DC(10204)
+ 0x1D(+29)	0x201D(8221)	0x203D(8253)	0x205D(8285)	0x27DD(10205)
+ 0x1E(+30)	0x201E(8222)	0x203E(8254)	0x205E(8286)	0x27DE(10206)
+ 0x1F(+31)	0x201F(8223)	0x203F(8255)	0x205F(8287)	0x27DF(10207)

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 words	Read input data this slot
+ 0x0B(+11) **	Read/Write	n words	Read/write output data this slot
+ 0x0E(+14)	Read	1 word	GT-number, if GT-1238, returns 0x1238
+ 0x0F(+15)	Read	String upto 72bytes	First 1 word 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 words	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 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.

5.4 MODBUS Reference

MODBUS Reference Documents

<http://www.modbus.org>

MODBUS Tools

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

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