
FnIO G-Series

GN-9386

GN-9386 (EtherCAT ID Type Network Adapter)

Table of Contents

1.Environment Specification.....	5
2.GN-9386 (EtherCAT ID Type Network Adapter).....	6
2.1.GN-9386 Specification.....	6
2.2.GN-9386 Wiring Diagram.....	7
2.3.GN-9386 LED Indicator.....	8
2.3.1.LED Indicator.....	8
2.3.2.MOD (Module Status LED).....	8
2.3.3.RUN (Current Running Status LED).....	8
2.3.4.ERROR (Error State LED).....	8
2.3.5.IOS LED (Extension Module Status LED).....	9
2.3.6.Field Power, System Power LED (Field Power, System Power Status LED).....	9
2.3.7.Indicator states and flash rates.....	9
2.4.GN-9386 Electrical Interface.....	10
2.4.1.RJ-45 Socket.....	10
2.4.2.DIP Switch.....	10
2.4.3.RS232 Port for MODBUS/RTU.....	10
2.5.EtherCAT ID Type Setup.....	11
2.5.1.Hot Connection On TwinCAT.....	11
2.6.I/O Process Image Map.....	13
2.6.1.Example of Input Process Image (Input Register) Map	14
2.6.2.Example of Output Process Image (Output Register) Map	15
3.EtherCAT Basics.....	16
3.1.EtherCAT State Machine.....	16
3.2.CoE Interface.....	18
3.2.1.parameter management in the EtherCAT system.....	18
3.2.2.Communication Objects.....	19
4.MODBUS Interface.....	21
4.1.MODBUS Interface Register/Bit Map.....	21
4.2.Supported MODBUS Function Codes.....	21
4.2.1.8 (0x08) Diagnostics.....	23
4.2.2.Error Response.....	24
4.3.MODBUS Special Register Map.....	25
4.3.1.Adapter Identification Special Register (0x1000, 4096).....	25
4.3.2.Adapter Information Special Register (0x1100, 4352).....	26

Specification

4.3.3.Expansion Slot Information Special Resister (0x2000, 8192).....	27
4.4.MODBUS Reference.....	28

Specification

History

Rev	Pages	Remarks	Date	Editor
1.00			May 26, 2016	DHLEE
1.00			Dec 15, 2016	Jeongmin, Lee
1.01		Hot connection / Modbus register updated	Jan 4, 2017	DHLEE
1.02		Modbus 0x1113 is removed / 0x1005 size is changed	Jan 9, 2017	DHLEE
1.03		SDO 0x1018 modification	July 27, 2017	DHLEE
1.05		Product name string length change	Dec 16, 2017	DHLEE
1.06		Master fault action, factory reset	Apr 6, 2018	GWLEE
1.07		IOS LED Status	Aug 28, 2018	GWLEE
1.08		ERR LED Status	Nov 21, 2018	GWLEE
1.09		Revision related to UL certification	Mar 10, 2020	GWLEE
1.09	26	Modbus special register map Update(0x1119)	July 07, 2020	Joonho, Park
1.10	6	Changed I/O Data Size	Sep 27, 2021	Joonho, Park
1.11	8	Added ERR LED Status	Mar 10, 2023	Joonho, Park
1.12	All		Aug. 25, 2023	Joonho, Park
1.13	10, 15, 28	Edited information about the RS232 port. Edited the order of Output Process Image Byte. Corrected incorrectly written content.	Apr. 29, 2024	Seonghyeon, Park
1.14	6	Changed I/O Data Size	June 17, 2024	Joonho, Park

Specification

1. Environment Specification

Environmental specification	
Operating Temperature	-40°C ~ 60°C
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

Specification

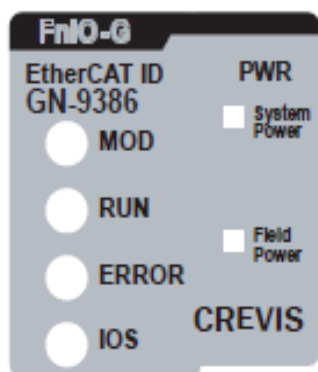
2. GN-9386 (EtherCAT ID Type Network Adapter)

2.1. GN-9386 Specification

Items	Specification
Communication Interface Specification	
Adapter Type	Slave Node (EtherCAT)
Max. Expansion Slot	63 slots
I/O Data Size	Max 128 bytes each slot
Max. Network Node	65,535
Baud Rate	100Mbps
Bus Connection	RJ-45 socket * 2pcs
Mac Address / IP Address	Not needed
Other Serial Port	RS232 for MODBUS/RTU, Touch Panel or IOGuide(Crevis Software)
Serial Configuration (RS232)	Node : 1 (Fixed) Baud Rate : 115200 (Fixed) Data bit : 8 (Fixed) Parity bit : No parity (Fixed) Stop bit : 1 (Fixed)
Indicator	6 Status LED 1 Green/Red, Module Status (MOD) 1 Green, Current Running Status (RUN) 1 Red, Error Status (ERROR) 1 Green/Red Expansion Module Status (IOS) 1 Green, System Power Status 1 Green, Field Power Status
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	Max. 70mA @ 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.
Wiring	I/O Cable Max. 2.0mm ² (AWG 14)
Weight	167g
Module Size	54mm x 99mm x 70mm
Environment Condition	Refer to '1. Environment Specification'

2.3. GN-9386 LED Indicator

2.3.1. LED Indicator



LED No.	LED Function / Description	LED Color
MOD	Module Status	Green/Red
RUN	Current Running Status	Green
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
Not Powered	OFF	power is not supplied to the unit.
Normal, Operational	Green	The unit is operating in normal condition.
Device in Standby	Flashing Green	The EEPROM parameter is not initialized yet. Serial Number is zero value (0x00000000)
Minor Fault	Flashing Red	The unit has occurred recoverable fault in self-testing. - EEPROM checksum fault.
Unrecoverable Fault	Red	The unit has occurred unrecoverable fault in self-testing. - Firmware fault

2.3.3. RUN (Current Running Status LED)

Status	LED	To indicate
Init	OFF	State of the EtherCAT State Machine: INIT = Initialization.
Pre-Operation	Blinking	State of the EtherCAT State Machine: PREOP = Pre-Operation.
Safe-Operation	Single Flash	State of the EtherCAT State Machine: SAFEOP = Safe-Operation.
Initialization or Bootstrap	Flashes	State of the EtherCAT State Machine: BOOT = Bootstrap (Update of the coupler firmware)
Operational	ON	State of the EtherCAT State Machine: Operational.

2.3.4. ERROR (Error State LED)

Status	LED	To indicate
No Error	OFF	No Error.
Invalid Configuration Communication Error	Blinking	Invalid Configuration. Communication Error.

Specification

2.3.5. IOS LED (Extension Module Status LED)

Status	LED	To indicate
Not Powered	OFF	Device has no expansion module or may not be powered.
Internal Bus On-line, Do not Exchanging I/O	Flashing Green	Internal Bus is normal but does not exchanging I/O data. (Passed the expansion module configuration)
Internal Bus Connection, Run Exchanging I/O	Green	Exchanging I/O data.
Internal Bus Connection Fault during Exchanging I/O	Red	One or more expansion module occurred in fault state. - Changed expansion module configuration. - Internal Bus communication failure. - Mismatch vendor code between adapter and expansion module.
Expansion Configuration Failed	Flashing Red	Failed to initialize expansion module. - Detect invalid expansion module ID. - Overflow Input/Output size. - No expansion module. - Too many expansion module. - Initial protocol failure.

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

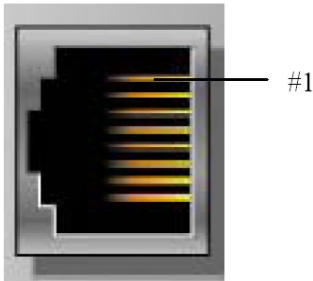
Status	LED	To indicate
Not supplied field, system power	OFF	Not supplied 24Vdc field power, 5Vdc system power.
Supplied field, system power	Green	Supplied 24Vdc field power, 5Vdc system power.

2.3.7. Indicator states and flash rates

LED ON	Constantly ON
LED OFF	Constantly OFF.
LED flickering	Equal ON and OFF times with a frequency of approximately 10 Hz: ON for approximately 50ms and OFF for approximately 50ms.
LED blinking	Equal ON and OFF times with a frequency of approximately 2, 5Hz: ON for approximately 200ms followed by OFF for approximately 200ms.
LED single flash	One short flash (approximately 200ms) followed by a long OFF phase (approximately 1000ms)
LED double flash	A sequence of two short flashes (approximately 200ms), separated by an OFF phase (approximately 200ms). The sequence is finished by a long OFF phase (approximately 1000ms)
LED triple flash	A sequence of three short flashes (approximately 200ms), separated by an OFF phase (approximately 200ms). The sequence is finished by a long OFF phase (approximately 1000ms)

2.4. GN-9386 Electrical Interface

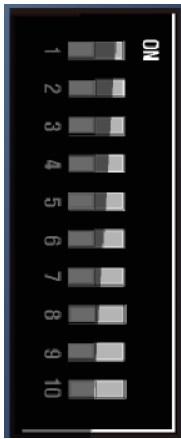
2.4.1. RJ-45 Socket



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	

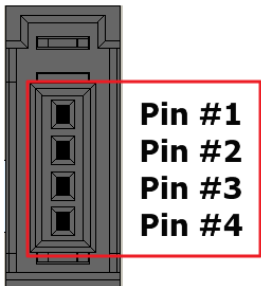
2.4.2. DIP Switch



DIP Pole#	Description
1	IdentificationValue DIP bit#0
2	IdentificationValue DIP bit#1
3	IdentificationValue DIP bit#2
4	IdentificationValue DIP bit#3
5	IdentificationValue DIP bit#4
6	IdentificationValue DIP bit#5
7	IdentificationValue DIP bit#6
8	IdentificationValue DIP bit#7
9	Not used
10	Not used

2.4.3. RS232 Port for MODBUS/RTU

The configuration interface used for the communication with IOGuidePro or for firmware download.



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

2.5. EtherCAT ID Type Setup

2.5.1. Hot Connection On TwinCAT

Hot connection function can be used to remove a node from a preconfigured Configuration or change the location of nodes and flexible. This feature is available only Ethercat ID Type in TwinCAT.

The user can use the external Dip Switch settings of the Adapter Identification Value.

For an example of using an external Dip Switch (Refer to 2.4.2.)

Ex) node 1 (Min)

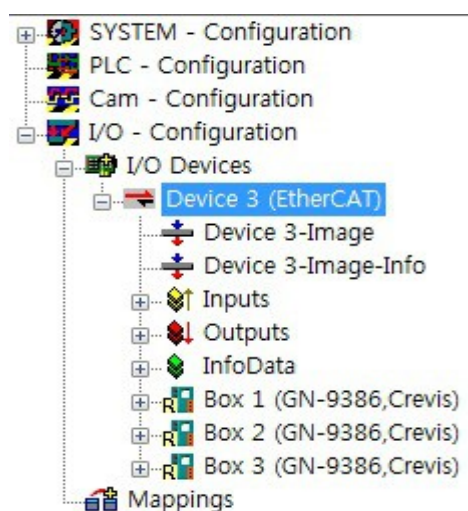


Ex) node 255 (Max)



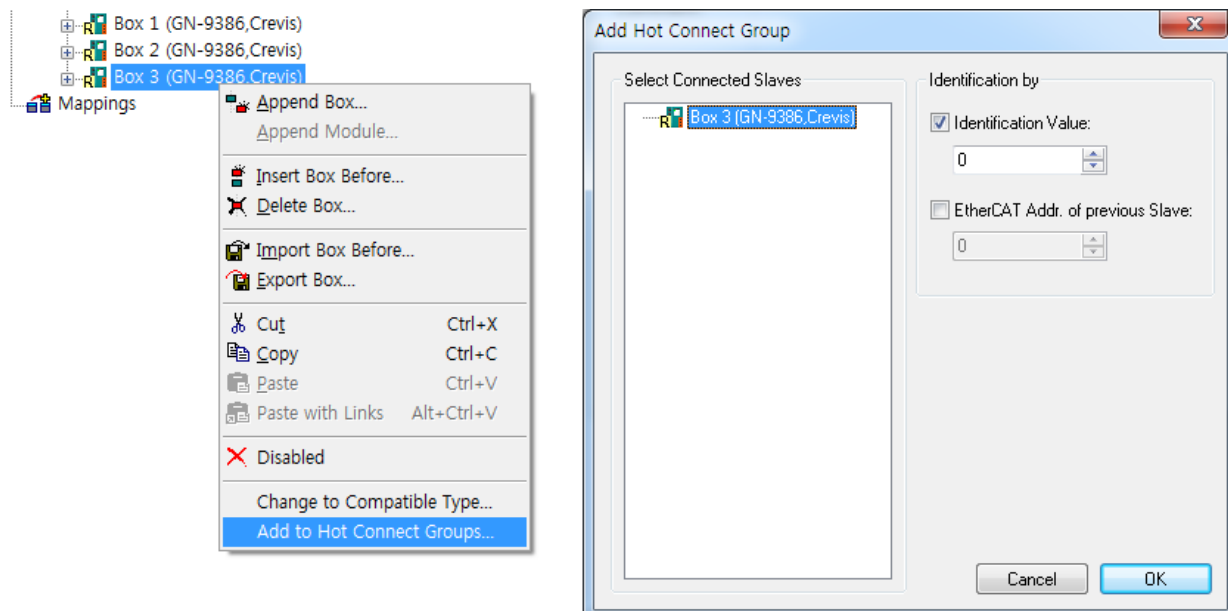
Hot Connection setting procedure.

1. Add the Ethercat ID Type in TwinCAT.

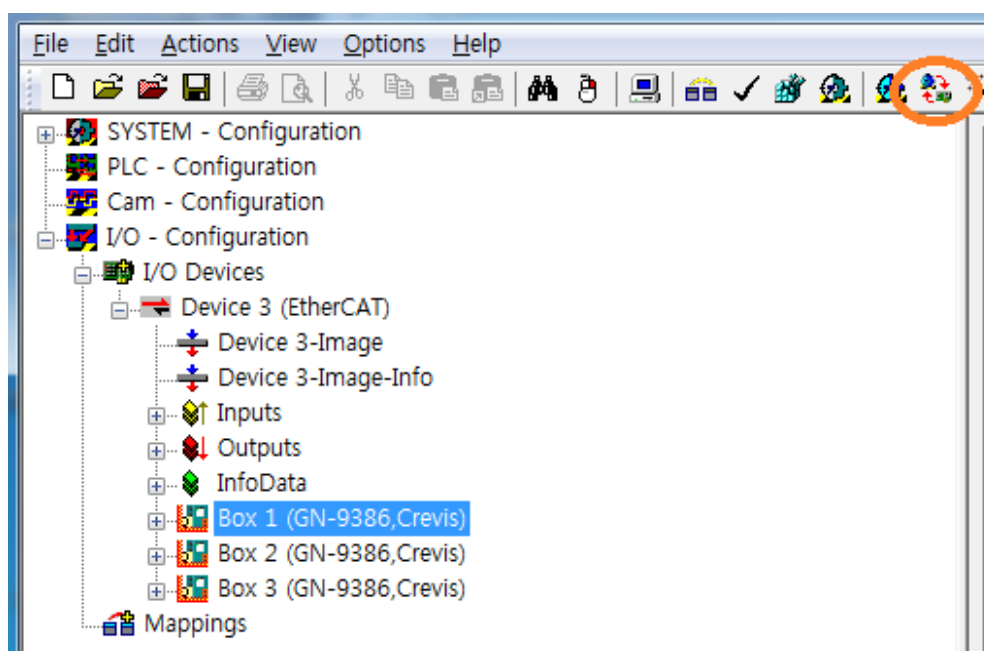


2. The Hot Connect Group settings.

Set the identification value same as dip-switch.



3. Hot connection group set up is completed, run the Reload I/O device(F4).



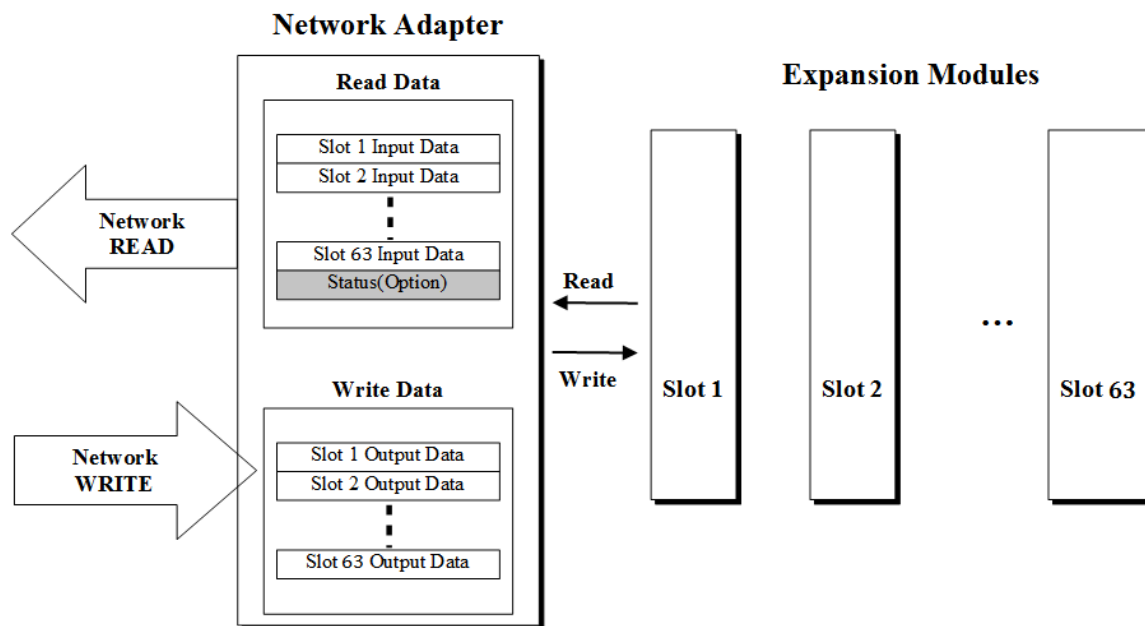
4. Now you can use the Hot connection feature.

Node is not overlapped between products. If there are same nodes, It should be changed.

2.6. 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.

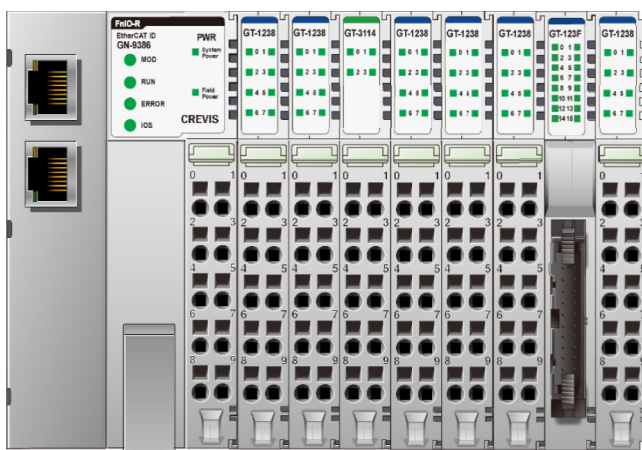


Specification

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

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

- For example slot configuration



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

- Input Process Image

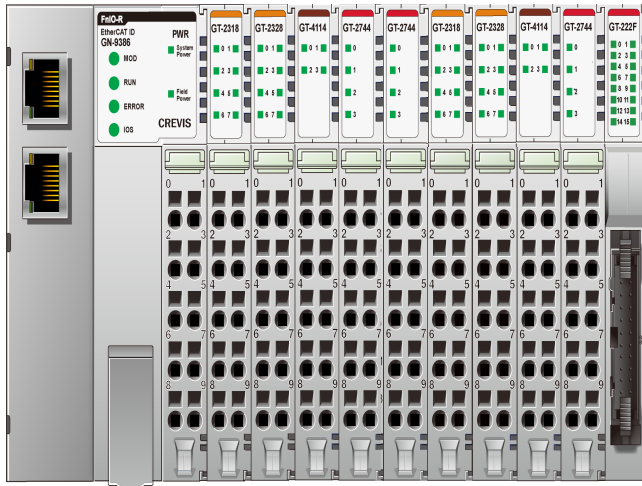
TXPDO	Entries	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x1A01	0x6010	0	Discrete Input 8 pts (Slot#1)							
0x1A02	0x6020	1	Discrete Input 8 pts (Slot#2)							
0x1A03	0x6030	2	Analog Input Ch0 low byte (Slot#3)							
		3	Analog Input Ch0 high byte (Slot#3)							
		4	Analog Input Ch1 low byte (Slot#3)							
		5	Analog Input Ch1 high byte (Slot#3)							
		6	Analog Input Ch2 low byte (Slot#3)							
		7	Analog Input Ch2 high byte (Slot#3)							
		8	Analog Input Ch3 low byte (Slot#3)							
		9	Analog Input Ch3 high byte (Slot#3)							
0x1A04	0x6040	10	Discrete Input 8 pts (Slot#4)							
0x1A05	0x6050	11	Discrete Input 8 pts (Slot#5)							
0x1A06	0x6060	12	Discrete Input 8 pts (Slot#6)							
0x1A07	0x6070	13	Discrete Input 8 pts (Slot#7)							
		14	Discrete Input 8 pts (Slot#7)							
0x1A08	0x6080	15	Discrete Input 8 pts (Slot#8)							

Specification

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

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

- For example slot configuration



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

- Output Process Image

RXPDO	Entries	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x1601	0x7010	0	Discrete Output 8 pts (Slot#1)							
0x1602	0x7020	1	Discrete Output 8 pts (Slot#2)							
0x1603	0x7030	2	Analog Output Ch0 low byte (Slot#3)							
		3	Analog Output Ch0 high byte (Slot#3)							
		4	Analog Output Ch1 low byte (Slot#3)							
		5	Analog Output Ch1 high byte (Slot#3)							
		6	Analog Output Ch2 low byte (Slot#3)							
		7	Analog Output Ch2 high byte (Slot#3)							
		8	Analog Output Ch3 low byte (Slot#3)							
		9	Analog Output Ch3 high byte (Slot#3)							
0x1604	0x7040	10	Discrete Output low 4 pts (Slot#4)							
0x1605	0x7050	11	Discrete Output low 4 pts (Slot#5)							
0x1606	0x7060	12	Discrete Output low 8 pts (Slot#6)							
0x1607	0x7070	13	Discrete Output low 8 pts (Slot#7)							
0x1608	0x7080	14	Analog Output Ch0 low byte (Slot#8)							
		15	Analog Output Ch0 high byte (Slot#8)							
		16	Analog Output Ch1 low byte (Slot#8)							
		17	Analog Output Ch1 high byte (Slot#8)							
		18	Analog Output Ch2 low byte (Slot#8)							
		19	Analog Output Ch2 high byte (Slot#8)							
		20	Analog Output Ch3 low byte (Slot#8)							
		21	Analog Output Ch3 high byte (Slot#8)							
0x1609	0x7090	22	Discrete Output low 8 pts (Slot#9)							
0x160A	0x70A0	23	Discrete Output low 8 pts (Slot#10)							
		24	Discrete Output high 8 pts (Slot#10)							

3. EtherCAT Basics

The EtherCAT protocol uses an officially assigned EtherType inside the Ethernet Frame. The use of this EtherType allows transport of control data directly within the Ethernet frame without redefining the standard Ethernet frame. The frame may consist of several sub-telegrams, each serving a particular memory area of the logical process images that can be up to 4 gigabytes in size. Addressing of the Ethernet terminals can be in any order because the data sequence is independent of the physical order. Broadcast, Multi-cast and communication between slaves are possible

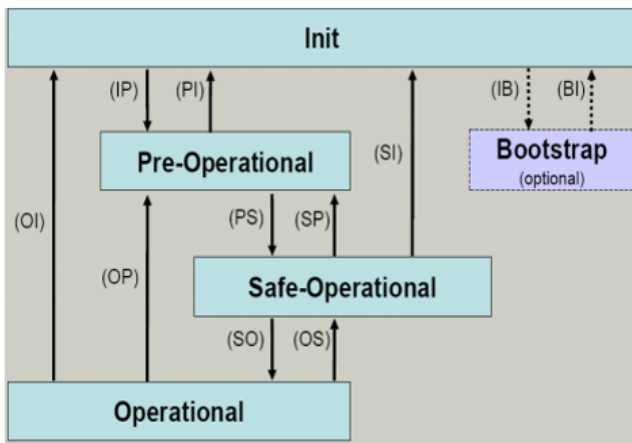
3.1. EtherCAT State Machine

The state of the EtherCAT slave is controlled via the EtherCAT State Machine (ESM). Depending upon the state, different functions are accessible or executable in the EtherCAT slave. Specific commands must be sent by the EtherCAT master to the device in each state, particularly during the boot up of the slave.

A distinction is made between the following states:

- Init
- Pre-Operational
- Safe-Operational and
- Operational
- Bootstrap

The regular state of each EtherCAT slave after bootup is the OP state.



Init

After switch-on the EtherCAT slave in the Init state. No mailbox or process data communication is possible.

The EtherCAT master initializes sync manager channels 0 and 1 for mailbox communication.

Pre-Operational (Pre-Op)

During the transition between Init and Pre-Op the EtherCAT slave checks whether the mailbox was initialized correctly.

In Pre-Op state mailbox communication is possible, but not process data communication. The EtherCAT master initializes the sync manager channels for process data (from sync manager channel 2), the FMMU channels and, if the slave supports configurable mapping, PDO mapping or the sync manager PDO assignment. In this state the settings for the process data transfer and perhaps terminal-specific parameters that may differ from the default settings are also transferred.

Safe-Operational (Safe-Op)

During transition between Pre-Op and Safe-Op the EtherCAT slave checks whether the sync manager channels for process data communication and, if required, the distributed clocks settings are correct. Before it acknowledges the change of state, the EtherCAT slave copies current input data into the associated DP-RAM areas of the EtherCAT slave controller (ECSC).

In Safe-Op state mailbox and process data communication is possible, although the slave keeps its outputs in a safe state, while the input data are updated cyclically.

Operational (Op)

Before the EtherCAT master switches the EtherCAT slave from Safe-Op to Op it must transfer valid output data.

In the Op state the slave copies the output data of the masters to its outputs. Process data and mailbox communication is possible.

Bootstrap

In the Boot state the slave firmware can be updated. The Boot state can only be reached via the Init state.

In the Boot state mailbox communication via the file access over EtherCAT (FoE) protocol is possible, but no other mailbox communication and no process data communication.

3.2. CoE Interface

3.2.1. parameter management in the EtherCAT system

The CiA organization (CAN in Automation) pursues among other things the goal of creating order and exchange ability between devices of the same type by the standardization of device descriptions. For this purpose so-called profiles are defined, which conclusively describe the changeable and unchangeable parameters of a device. Such a parameter encompasses at least the following characteristics:

- Index number – for the unambiguous identification of all parameters. The index number is divided into a main index and a subindex in order to mark and arrange associated parameters.
 - Main index
 - Subindex, offset by a colon ‘:’
- Official name – in the form of an understandable, self-descriptive text
- Specification of changeability, e.g. whether it can only be read or can also be written
- A value – depending upon the parameter the value can be a text, a number or another parameter index.

Index Range

The relevant ranges for EtherCAT fieldbus users are:

x1000 : This is where fixed identity information for the device is stored, including name, manufacturer, serial number etc., plus information about the current and available process data configurations.

x8000 : This is where the operational and functional parameters for all channels are stored, such as filter settings or output frequency.

Other important ranges are:

x4000 : In some EtherCAT devices the channel parameters are stored here (as an alternative to the x8000 range).

x6000 : Input PDOs ("input" from the perspective of the EtherCAT master)

x7000 : Output PDOs ("output" from the perspective of the EtherCAT master)

Specification

3.2.2. Communication Objects

Index	Sub-index	Name	Flags	Default value
1000		Device type	RO	0x00001389
1001		Gbus Status	RO	Normal Operation : 0x00 **
1002		Master Fault Aaction	RW	0x00
1008		Device name	RO	GN-9386(Crevis)
1009		Hardware version	RO	GN-9386.v1
100A		Software version	RO	1.000
1018	Identity		RO	0x05
	01	Vendor ID (Crevis: 029D)	RO	0x0000029D
	02	Product code	RO	0x4E419386
	03	Revision	RO	0x0001000
	04*	Serial number	RO	0xFFFFFFFF
	05	Release date	RO	0x20160823
10F1	Error Settings		RO	0x02
	01	Local Error Reaction	RO	0x00000000
	02	Sync Error Counter Limit	RO	0x00000004
1601*	Slot#x, GT-xxxx,RXPDO		RO	0xnn
	01	SubIndex 001	RO	0x7010:01, 8

	nn	SubIndex nnn	RO	0x7010:nn, 8
1A01*	Slot#x, GT-xxxx,TXPDO		RO	0xnn
	01	SubIndex 001	RO	0x6010:01, 8

	nn	SubIndex nnn	RO	0x6010:nn, 8
1C00	Sync manager type		RO	0x04
	01	SubIndex 001	RO	0x01
	02	SubIndex 002	RO	0x02
	03	SubIndex 003	RO	0x03
	04	SubIndex 004	RO	0x04
1C12	RxPDO assign		RO	0x01
	01	SubIndex 001	RO	0x1601
1C13	TxPDO assign		RO	0x02
	01	SubIndex 001	RO	0x1A01
	02	SubIndex 002	RO	0x1A02
7010*	GT-xxxx		RO	0xnn
	01	Byte#0	RW P	0x00

	nn	Byte#nnn	RW P	0x00
8000	GN-9386(Parameter)		RO	
	01	Byte#0	RW	
	02	Byte#1	RW	
	03	Byte#2	RW	
	04	Byte#3	RW	
8nn0*	GT-xxxx(Parameter)		RO	
	01	Byte#0	RW	

	nn	Byte#nnn	RW	
F000	Module device profile		RO	
	01	Module index distance	RO	
	02	Maximum numver of modules	RO	
F010*	Module List		RO	
	01	Subindex 001 (GN-9386)	RO	0x00009386

	63	Subindex 063	RO	0x0000xxxx
F050	Detected Module Ident List		RO	
	01...	SubIndex 001	RO	

*This value can be changed depending on the configuration of expansion modules

** Gbus Status

- Normal Operation : 0x00
- Communication Fault : 0x02
- Configuration Failed : 0x03
- No Expansion Module : 0x04
- Vendor Error : 0x07
- Not expected slot : 0x08
- CRC Error : 0x09

4. MODBUS Interface

4.1. 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

4.2. 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.

Specification

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

4.2.1. 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

4.2.2. 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.

4.3. 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).

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

Address	Access	Type, Size	Description
0x1000(4096)	Read	1word	Vendor ID = 0x029D(669), Crevis. Co., Ltd.
0x1001(4097)	Read	1word	Device type = 0x000C, Network Adapter
0x1002(4098)	Read	1word	Product Code = 0x9010
0x1003(4099)	Read	1word	Firmware revision, if 0x0100, revision 1.00
0x1004(4100)	Read	2words	Product unique serial number
0x1005(4101)	Read	String upto 36bytes	Product name string (ASCII) “GN-9386,EtherCAT ID Type,G-Series”
0x1006(4102)	Read	1word	Sum check of EEPROM
0x1010(4112)	Read	2words	Firmware release date
0x101E(4126)	Read	7words - 1word - 1word - 1word - 1word - 1word - 2words	Composite Id of following address 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

Specification

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

Address	Access	Type, Size	Description	
0x1100(4352)	Read/ Write	1word	Master fault action option. - 0x00 : Normal option - 0x01 : Master fault action This option can enable Master fault action option. With master fault action, fault action can be activated with master communication failure. Also, can activate hold last state as IO parameter.	
0x1102(4354)	Read	1word	Start address of input image word register. =0x0000	
0x1103(4355)	Read	1word	Start address of output image word register. =0x0800	
0x1104(4356)	Read	1word	Size of input image word register.	
0x1105(4357)	Read	1word	Size of output image word register.	
0x1106(4358)	Read	1word	Start address of input image bit. = 0x0000	
0x1107(4359)	Read	1word	Start address of output image bit. =0x1000	
0x1108(4360)	Read	1word	Size of input image bit.	
0x1109(4361)	Read	1word	Size of output image bit.	
0x110D(4365)	Read	1word	Current Dip Switch Value and Field Power Status (MSB) ex) Field Power ON, Dip Switch 0x03 = 0x8003	
0x110E(4366)	Read	upto 33words	Expansion slot's GT-number including GN First 1word is adapter's number, if GN-9386, then 0x9386	
0x1110(4368)	Read	1word	Number of expansion slot	
0x1119(4377)	Read	1word	High byte is ModBus status, low byte is internal bus status. Zero value means 'no error'.	
			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

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

Specification

4.3.3. 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	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 up to 74bytes	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, up to 8byte. Refer to each IO parameter Specification.
+ 0x17(+23)	Read	2words	Firmware Revision ex) 0x00010010 (Major revision 1 / Minor revision 16, Rev 1.016)
+ 0x19(+25)	Read	2words	Firmware release date.

** Nothing of output, input, memory or configuration parameter corresponding slot returns Exception 02.(refer to 4.2.2)

4.4. MODBUS Reference

MODBUS Reference Documents

<http://www.modbus.org>

MODBUS Tools

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

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