

# MODBUS<sup>®</sup> TCP/IP for H2–EBC100

---

## In This Chapter. . . .

- MODBUS TCP/IP
  - Supported MODBUS Function Codes
  - MODBUS 584/984 Addressing
  - H2–EBC100 System Memory
  - Current / Last State Error Codes
-

## MODBUS TCP/IP

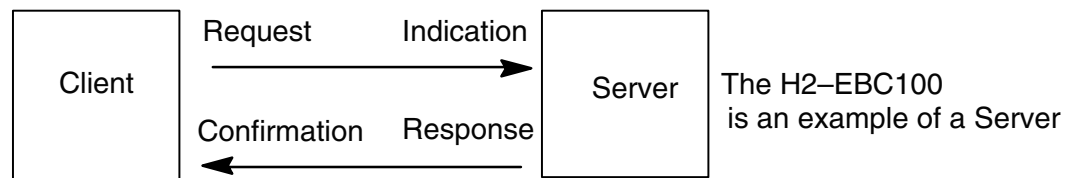
MODBUS TCP/IP is essentially the serial MODBUS RTU protocol encapsulated in a TCP/IP wrapper. MODBUS RTU is used for serial communications between a master and slave(s) devices. MODBUS TCP/IP is used for TCP/IP communications between client and server devices on an Ethernet network. The TCP/IP version of Modbus follows the OSI Network Reference Model.

### Client / Server Model

The MODBUS messaging service provides a Client/Server communication between devices connected on an Ethernet TCP/IP network. This client / server model is based on four type of messages:

- MODBUS Request – the message sent on the network by the Client to initiate a transaction
- MODBUS Confirmation – the Response Message received on the Client side
- MODBUS Indication – the Request message received on the Server side
- MODBUS Response – the Response message sent by the Server

### Client / Server Model



### Protocol Description

A typical MODBUS TCP/IP frame consists of the following fields:



The **MBAP header** (MODBUS Application Protocol header) is seven bytes long. It consists of the following fields.

- Transaction Identifier – It is used for transaction pairing, the MODBUS server copies in the response the transaction identifier of the request. (2 bytes)
- Protocol Identifier – It is used for intra-system multiplexing. The MODBUS protocol is identified by the value 0. (2 bytes)
- Length – The length field is a byte count of the following fields, including the Unit Identifier and data fields. (2 bytes)
- Unit Identifier – This field is used for intra-system routing purpose. It is typically used to communicate to a MODBUS or a MODBUS+ serial line slave through a gateway between an Ethernet TCP/IP network and a MODBUS serial line. This field is set by the MODBUS Client in the request and must be returned with the same value in the response by the server. (1 byte)

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

- The MODBUS “slave address” field usually used on MODBUS Serial Line is replaced by a single byte “Unit Identifier” within the MBAP Header. The “Unit Identifier” is used to communicate via devices such as bridges, routers and gateways that use a single IP address to support multiple independent MODBUS end units.
- All MODBUS requests and responses are designed in such a way that the recipient can verify that a message is finished. For function codes where the MODBUS PDU has a fixed length, the function code alone is sufficient. For function codes carrying a variable amount of data in the request or response, the data field includes a byte count.
- Protocol Identifier – It is used for intra-system multiplexing. The MODBUS protocol is identified by the value 0. (2 bytes)

The **function code field** of a message contains 8 bits. Valid function codes are in the range of 1 – 255 decimal. The function code instructs the slave what kind of action to take. Some examples are to read the status of a group of discrete inputs; to read the data in a group of registers; to write to an output coil or a group of registers; or to read the diagnostic status of a slave.

When a slave responds to the master, it uses the function code field to indicate either a normal response or that some type of error has occurred. For a normal response, the slave echoes the original function code. In an error condition, the slave echoes the original function code with its MSB set to a logic 1.

The **data field** is constructed using sets of two hexadecimal digits in the range of 00 to FF. According to the network’s serial transmission mode, these digits can be made of a pair of ASCII characters or from one RTU character.

The data field also contains additional information that the slave uses to execute the action defined by the function code. This can include internal addresses, quantity of items to be handled, etc.

The data field of a response from a slave to a master contains the data requested if no error occurs. If an error occurs, the field contains an exception code that the master uses to determine the next action to be taken. The data field can be nonexistent in certain types of messages.



**Note:** ModScan32 is a Windows based application program that can be used as a MODBUS master to access and change data points in a connected slave/server device (H2–EBC100) The utility is ideally suited for quick and easy testing of MODBUS TCP network slave devices. Visit [www.win-tech.com](http://www.win-tech.com) to download a free ModScan32 trial demo and for more information on ModScan32.

## Supported MODBUS Function Codes

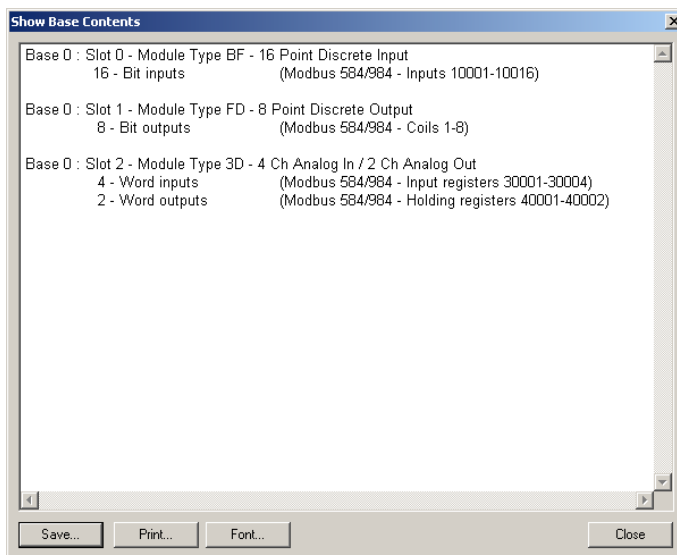
The following MODBUS function codes are supported by the H2–EBC100 base controller.

MODBUS Function Code	Function
01	Read Output Table
02	Read Input Table
03	Read Holding Registers (when addressing mode is 584/984, this function is used to access analog output registers)
04	Read Input Registers (when addressing mode is 584/984, this function is used to access analog input registers)
05	Force Single Output
06	Preset Single Registers
08	Loop back / Maintenance
15	Force Multiple Outputs
16	Preset Multiple Registers

## MODBUS 584/984 Addressing

Modbus Data Type (Bit)		H2-EBC100				
		Range (Decimal)	Points	Memory Type	Access	
Coil		1 – 1024	1024	Discrete Output	R/W	
		1025 – 10000	–	Reserved	–	
Input		10001 – 11024	1024	Discrete Input	R only	
		11025 – 20000	–	Reserved		
Modbus Data Type (Word)		Range (Decimal)	Words (16– bit)	Channel (32– bit)	Memory Type	
Input Register	Analog Input	30001 – 30512	512	256	Analog Input Register	R only
	Input Register	30513 – 32000	–	–	Reserved	–
	Bit Input Register	32001 – 32064	64	32	Discrete Input Bit Register	R only
	Input Register	32065 – 37000	–	–	Reserved	–
Hold Register	Analog output	40001 – 40512	512	256	Analog Output Register	R/W
	Hold Register	40513 – 42000	–	–	Reserved	–
	Bit Output Register	42001 – 42064	64	32	Discrete Output Bit Register	R/W
	Hold Register	42065 – 44000	–	–	Reserved	–

Note: NetEdit3 Show Base Contents function will list the MODBUS addressing for each I/O module on the base. For the analog I/O, the module Configuration Data registers are also listed. Refer to Chapter 3 for information on NetEdit3.



## MODBUS 584/984 Addressing for Function Code 3 Clients

This memory map offers duplicate registers from the 30001 range and Bit memory data type into the 411000 range for clients/masters that only support function code 3. These ranges are word level data only.

Modbus Word Data Type		H2-EBC100				
		Range (Decimal)	Words	Memory Type	Access	
Coil		411000 – 411063	64		Discrete Output	R/W
		411064 – 411124	–		Reserved	–
Input		411625 – 411688	64		Discrete Input	R only
		411689 – 412062	–		Reserved	
Modbus Word Data Type		Range (Decimal)	Words (16-bit)	Channel (32-bit)	Memory Type	
Input Register	Analog Input	412251 – 412762	512	256	Analog Input Register	R only
	Input Register	412763 – 414250	–	–	Reserved	–
	Bit Input Register	414251 – 414314	64	32	Discrete Input Bit Register	R only
	Input Register	414315 – 419250	–	–	Reserved	–
Hold Register	Analog output	40001 – 40512	512	256	Analog Output Register	R/W
	Hold Register	40513 – 42000	–	–	Reserved	–
	Bit Output Register	42001 – 42064	64	32	Discrete Output Bit Register	R/W
	Hold Register	42065 – 44000	–	–	Reserved	–

## H2-EBC100 System Memory

	H2-EBC100			
	Modbus Addressing Range (Decimal)	Words (16-bit)	Word Descriptions	Access
<b>Module Version Information</b>	<b>37001 – 37006</b> <b>(419251 – 419256)*</b>	6	1 – OS Major Version 2 – OS Minor Version 3 – OS Build Version 4 – Booter Major Version 5 – Booter Minor Version 6 – Booter Build Version	R only
	37007 – 37010 (419257 – 419260)	–	Reserved	–
<b>Device Data</b>	<b>37011 – 37100</b> <b>(419261 – 419350)*</b>	90	1 – Version of Device 2 – Family 3 – Processor 4 – Module Type 5 – Status Code (6–8) – Ethernet Address 9 – RAM Size 10 – Flash Size 11 – Batt Switch 12 – DIP Settings 13 – Media Type (14–15) – Reserved 16 – Reserved 17 – Reserved 18 – Model Number 19 – Ethernet Speed 20 – Reserved 21 – IO Total Byte Count 22 – Bit Input Byte Count 23 – Bit Output Byte Count 24 – Non-bit Input Byte Count 25 – Non-bit Output Byte Count (26–90) – Reserved	R only
<b>I/O Module ID's</b>	<b>37101 – 37108</b> <b>(419351 – 419358)*</b>	8 (1 word per slot)	I/O module ID numbers per slot location	R only
	37133 – 37200 (419359 – 419450)	–	Reserved	–
<b>Module Information</b>	<b>37201 – 37232</b> <b>(419451 – 419482)*</b>	32 (4 words per slot)	1 – Bit Input Count 2 – Bit Output Count 3 – Non-bit Input Count 4 – Non-bit Output Count	R only
	37329 – 37400 (419483 – 419650)	–	Reserved	–

\*For clients that only support function code 3 to read word data.

## H2-EBC100 System Memory (continued)

	H2-EBC100			
	Modbus Addressing Range (Decimal)	Words (16-bit)	Word Descriptions	Access
<b>EBC Dynamic Module Data</b>	410001 – 410020	20	1 – See Error Codes on p. 4–9. 2 – Error bit–per–slot for first 16 slots If any bit is set, see extended error info of Module Status data for specific problem 3 – Error bit–per–slot for second 16 slots (if present) If any bit is set, see extended error info of Module Status data for specific problem NOTE: Any write to [1], [2], or [3] above will clear the module / slot errors. 4 – Flags: Bit 0: If 1, module has rebooted since this bit was cleared, a write to the Flags word with this bit set will clear this reboot bit. Bit 1 – 15: Reserved 5 – Reboot Count (LSW) – Read Only 6 – Reboot Count (MSW) – Read Only 7 – Link Monitor Timeout (EBC communication watchdog Timer) – 0 to disable; range 0 – 10000ms. 8–20 – Reserved	R / W
	410021 – 410052	–	Reserved	–
<b>I/O Module Status</b>	<b>37401 – 37560</b> <b>(419651 – 419810)*</b>	160 (20 words per slot)	1 – Flags with bits indicating presence of Error, Warning, Info Values Bit 0: If set, indicates that Error Value is non-zero Bit 1: If set, indicates that Warning Value is non-zero Bit 2: If set, indicates that Info Value is non-zero Bit 3: Reserved Bit 4: If set, indicates that Extended error info is present Bit 5: Reserved Bit 6: Reserved Bit 7: Reserved For Words 2–4, refer to Current/Last State Error Codes Table on page 4–9. 2 – Error Code 3 – Warning Code 4 – Info Code 5 – 20: Reserved	R only
	37561 – 40000 (419811 – 422250)	–	Reserved	–

\*For clients that only support function code 3 to read word data.



## Current / Last State Error Codes

The following table lists the error codes for Words 2–4 in the **Module Status** System Memory area.

Error Code (Decimal)	Description
E0	No error.
E121	Channel failure.
E122	Unused analog input channels exist.
E139	Broken transmitter on one of the analog input channels (if supported by analog module)
E142	Multiple channels failed.
E154	I/O configuration has changed. See E153 for reset methods.
E200– E216	Unused analog input channels exist at channel xx (1–16), where xx = Value –200. (example: E212 indicates unused analog channel exists at channel 12.)

## Extended Error Codes

The following table lists the error codes for Words 5–20 in the **Module Status** System Memory area.

Error Code (Decimal)	Description														
E32– E63	Bitwise error where bit 5 is always SET. Look at bit 0 thru bit 4 to get a possible list of errors. Example 34 decimal =22 hexadecimal (Bit 5 SET and Bit 1 SET). <table border="1" data-bbox="552 976 1266 1176"> <thead> <tr> <th>BIT</th> <th>Type of Error</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Terminal block off</td> </tr> <tr> <td>1</td> <td>External P/S voltage low</td> </tr> <tr> <td>2</td> <td>Fuse blown</td> </tr> <tr> <td>3</td> <td>Bus error</td> </tr> <tr> <td>4</td> <td>Module initialization error (intelligent module)</td> </tr> <tr> <td>5</td> <td>Fault exists in module (this bit is SET if any of the above bits are SET)</td> </tr> </tbody> </table>	BIT	Type of Error	0	Terminal block off	1	External P/S voltage low	2	Fuse blown	3	Bus error	4	Module initialization error (intelligent module)	5	Fault exists in module (this bit is SET if any of the above bits are SET)
BIT	Type of Error														
0	Terminal block off														
1	External P/S voltage low														
2	Fuse blown														
3	Bus error														
4	Module initialization error (intelligent module)														
5	Fault exists in module (this bit is SET if any of the above bits are SET)														
E117	Write attempt to an invalid analog channel.														
E119	Data not valid. Subnet mask or IP address not allowed // EBC SDK data packet not constructed properly.														
E121	Analog input channel error.														
E122	Unused analog input channels exist.														
E139	Broken transmitter on one of the analog input channels.														
E142	Channel failure.														
E200– E216	Unused analog input channels exist at channel xx (1–16), where xx = Value –200.														