4

Modbus® TCP for T1H-EBC100

In This Chapter. . . .

- Modbus TCP/IP
- Supported Modbus Function Codes
- Modbus 584/984 Addressing
- Modbus 584/984 Addressing for Function 3 Clients
- T1H-EBC100 System Memory
- Current / Last State Error Codes
- Extended Error Codes
- Analog Input Module Configuration
- Analog Output Module Configuration

Modbus TCP

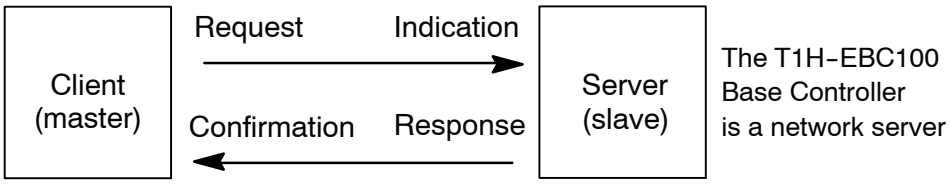
Modbus TCP is essentially the serial MODBUS RTU protocol encapsulated in a TCP/IP wrapper. Modbus RTU is used for serial communications between a master and slave(s) devices. Modbus TCP is used for TCP communications between client and server devices on an Ethernet network. The TCP version of Modbus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

The MBAP 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.

ModScan32 is a Windows based application program that can be used as a Modbus master (client) to access and change data points in a connected slave (server) device (i.e. T1H-EBC100).
The utility is ideally suited for quick and easy testing of Modbus TCP network server devices. Visit www.win-tech.com to download a free ModScan32 trial demo and for more information on ModScan32.

Supported Modbus Function Codes

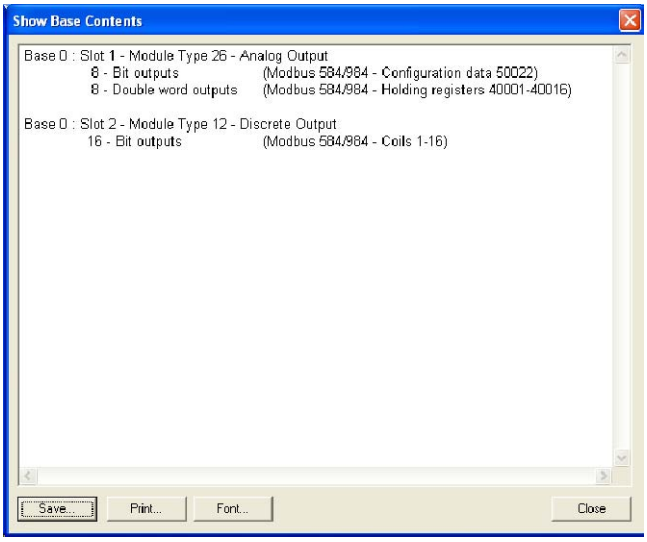
The following Modbus function codes are supported by the T1H-EBC100 base controller.

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		T1H-EBC100				
		Range (Decimal)	Points		Memory Type	Access
Coil		**1 - 1024**	1024		**Discrete Output**	Read / Write
		1025 – 10000	–		Reserved	–
Input		**10001 - 11024**	1024		**Discrete Input**	Read only
		11025 – 20000	–		Reserved	
Modbus Data Type						
		Range (Decimal)	**Words (16-bit)**	**Channel (32-bit)**	**Memory Type**	
Input Register	**Analog Input (see table below)**	**30001 - 30512**	512	256	Analog Input Register	Read only
	Input Register	30513 – 32000	–	–	Reserved	–
	Bit Input Register	**32001 - 32064**	64	32	Discrete Input Bit Register	Read only
	Input Register	32065 – 37000	–	–	Reserved	–
Hold Register	**Analog output (see table below)**	**40001 - 40512**	512	256	Analog Output Register	Read / Write
	Hold Register	40513 – 42000	–	–	Reserved	–
	Bit Output Register	**42001 - 42064**	64	32	Discrete Output Bit Register	Read / Write
	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

The following 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		T1H-EBC100				
		Range (Decimal)	Words		Memory Type	Access
Coil		**411000 - 411063**	64		**Discrete Output**	Read / Write
		411064 – 411124	–		Reserved	–
Input		**411625 - 411688**	64		**Discrete Input**	Read only
		411689 – 412062	–		Reserved	
Modbus Word Data Type		**Range (Decimal)**	**Words (16-bit)**	**Channel (32-bit)**	**Memory Type**	
Input Register	**Analog Input (see table below)**	**412251 - 412762**	512	256	Analog Input Register	Read only
	Input Register	412763 – 414250	–	–	Reserved	–
	Bit Input Register	**414251 - 414314**	64	32	Discrete Input Bit Register	Read only
	Input Register	414315 – 419250	–	–	Reserved	–
Hold Register	**Analog output (see table below)**	**40001 - 40512**	512	256	Analog Output Register	Read / Write
	Hold Register	40513 – 42000	–	–	Reserved	–
	Bit Output Register	**42001 - 42064**	64	32	Discrete Output Bit Register	Read / Write
	Hold Register	42065 – 44000	–	–	Reserved	–

T1H-EBC100 System Memory

	T1H-EBC100			
	Modbus Addressing Range (Decimal)	**Words (16-bit)**	**Word Descriptions**	**Access**
Module Version Information	**37001 - 37006 (419251 - 419256)***	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	-
Device Data	**37011 - 37100 (419261 - 419350)***	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
I/O Module ID's	**37101 - 37132 (419351 - 419382)***	32 (1 word per slot)	I/O module ID numbers per slot location	R only
	37133 - 37200 (419383 - 419450)	-	Reserved	-
Module Information	**37201 - 37328 (419451 - 419578)***	128 (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 (419579 - 419650)	-	Reserved	-

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

(continued)

T1H-EBC100 System Memory (continued)

	T1H-EBC100			
	Modbus Addressing Range (Decimal)	**Words (16-bit)**	**Word Descriptions**	**Access**
EBC Dynamic Module Data	**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: Write Only Bit - A write to the Flags word with this bit set will cause the base to be re-scanned. Bit 2: Write Only Bit - If Bit 1 is set to do rescan, this bit is used to indicated if RESCAN_LEAVE_IMAGE_RAM or RESCAN_CLEAR_IMAGE_RAM Bit 3-7: Reserved 5 - Reboot Count (LSW) - Read Only 6 - Reboot Count (MSW) - Read Only 7 - Link Monitor Timeout - 0 to disable 8-20 - Reserved	R / W
Configuration Data	**410021 - 410052**	32	1 word per slot to read/write module configuration data (See Analog I/O Module Configuration tables at the end of this chapter for bit definitions)	R / W
	410053 - 425536	-	Reserved	-

(continued)

T1H-EBC100 System Memory (continued)

	T1H-EBC100			
	Modbus Addressing Range (Decimal)	**Words (16-bit)**	**Word Descriptions**	**Access**
I/O Module Status	**37401 - 38040 (419651 - 420290)***	640 (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 (p.4-9) 2 - Error Code 3 - Warning Code 4 - Info Code For Words 5-20, refer to Extended Error Codes Table (p.4-9) 5 - Extended Error Code 1 (i.e channel 1 of an analog module) 6 - Extended Error Code 2 (i.e channel 2 of an analog module) 7 - Extended Error Code 3 (i.e channel 3 of an analog module) 8 - Extended Error Code 4 (i.e channel 4 of an analog module) 9 - Extended Error Code 5 (i.e channel 5 of an analog module) 10 - Extended Error Code 6 (i.e channel 6 of an analog module) 11 - Extended Error Code 7 (i.e channel 7 of an analog module) 12 - Extended Error Code 8 (i.e channel 8 of an analog module) 13 - Extended Error Code 9 (i.e channel 9 of an analog module) 14 - Extended Error Code 10 (i.e channel 10 of an analog module) 15 - Extended Error Code 11 (i.e channel 11 of an analog module) 16 - Extended Error Code 12 (i.e channel 12 of an analog module) 17 - Extended Error Code 13 (i.e channel 13 of an analog module) 18 - Extended Error Code 14 (i.e channel 14 of an analog module) 19 - Extended Error Code 15 (i.e channel 15 of an analog module) 20 - Extended Error Code 16 (i.e. channel 16 of an analog module)	R only
	38041 - 40000 (420291 - 422250)	-	Reserved	-

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

(continued)

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.
E153	The module which was in this slot is no longer responding. User has removed a module in a Terminator I/O slave system. If Automatic Reset (default) is enabled for this slave, it will reset itself once the replacement module is inserted. If Manual Reset is enabled for this slave, the user must 1) SET the slave disable flag for that slave in the first diagnostic output word, 2) wait for bits 8-15 in second diagnostic input word to equal 1, then 3) RESET the slave disable flag in the first diagnostic output word.
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). 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.
E146	Communications failure. Hitachi drive on-board relay set.
E153	The module which was in this slot is no longer responding. User has removed a module in a Terminator I/O slave system. If Automatic Reset is enabled for this slave, it will reset itself once the replacement module is inserted. If Manual Reset is enabled for this slave, the user must 1) SET the slave disable flag for that slave in the first diagnostic output word, 2) wait for bits 12-15 in second diagnostic input word to equal 1, then 3) RESET the slave disable flag in the first diagnostic output word.
E154	One or more new modules has been inserted into the base. See E153 for reset methods.
E155	Terminator module status error. One or more of the modules in the T1H-EBC100 base has an error. For more detail check extended errors
E200-E216	Unused analog input channels exist at channel xx (1-16), where xx = Value -200.

Analog Input Module Configuration

The Terminator I/O analog input modules are configured using the following bit definitions located in the Configuration Data memory area of the T1H-EBC100's System Memory. Only the T1F-08AD1 and T1F-08AD2 support Fast Response mode.

Analog Input Module Configuration Bits		
Bit 0-4	**Input Enable** 0 = All Channels Enabled 1 - 31 = Number of Channels Enabled Starting With Channel 1	Write
Bit 5-6	Reserved	-
Bit 7	0 = Normal Response 1 = Fast Response **(T1F-08AD1 and T1F-08AD2 only)**	Write
Bit 8-15	Reserved	-

Analog Output Module Configuration

The Terminator I/O analog output modules are configured using the following bit definitions located in the Configuration Data memory area of the T1H-EBC100's System Memory.

Analog Output Module Configuration Bits		
Bit 0	**Outputs Enable** 0 = All outputs OFF 1 = All outputs Enabled	Write
Bit 1	**Unipolar** / **Bipolar** 0 = Unipolar selected 1 = Bipolar selected	Write
Bit 2	**5V** / **10V Range** 0 = 5V range 1 = 10V range	Write
Bit 3	**0 - 20mA** / **4-20mA Range** 0 = 0 - 20mA range 1 = 4 - 20mA range	Write
Bit 4-15	Reserved	-