
MODBUS PROTOCOL EMULATION

1.1 GENERAL DESCRIPTION

This section briefly describes the MODBUS communication protocol for reference purposes only. The appropriate MODICON documentation should be consulted for complete details of the MODBUS protocol.

The MODBUS standard protocol is an asynchronous protocol designed to connect directly to computer communication ports. The protocol may be used either in a point-to-point or in a multi-drop configuration. The protocol can be used in either half or full-duplex operation. Communications security is provided by a 16-bit calculated cyclic redundancy check (CRC) when used in the "RTU" mode and by an 8-bit LRC check byte when used in the "ASCII" mode.

All communications exchanges in MODBUS protocol are initiated by the host. The remote cannot initiate any exchange with the host nor can the remote directly address or communicate with another remote. The remote will return a response to the host for all valid messages sent by the host and addressed to the remote. The only exception to this is in broadcast (all station) messages which produce no response from any remote. Also, all messages received by the remote are validated by checking the header and trailer bytes. If these bytes are not valid, the remote will ignore the message; no action or response will be initiated.

1.2 MESSAGE STRUCTURE

1.2.1 MODBUS ASCII Mode

In the ASCII mode of operation each byte of information which is sent is first divided into two 4-bit parts. Each 4-bit part (nibble) is then replaced by the ASCII character equal to the nibble's hexadecimal equivalent (0-9, A-F). The message streams thus consist entirely of printable ASCII characters.

All messages consist of a header, data as required by the function code, and a trailer. The header consists of three bytes. The first byte is the sync byte. This byte will always be the colon character ":". The second byte of the header is the MODBUS address. This is a unique hardware unit number assigned to each remote device. Valid addresses are 1-255 with 0 reserved as the broadcast address. The third byte of the

APPENDIX C

MODBUS PROTOCOL EMULATION

C-2
Rev. 1

header is the MODBUS function code. This function code may range from 0 to 255; however, not all possible function codes are currently used. Figure C-1 details the MODBUS function codes and identifies those that are currently implemented in the Comm-Troller.

Function Code	Description	Implemented
1	Read Coil (output) Status	Y
2	Read Input Status	Y
3	Read Holding Register	Y
4	Read Input Registers	Y
5	Force Single Coil	Y
6	Preset Single Register	Y
7	Read Exception Status	N
8	Loopback Diagnostic Test	Y
9	Program (484 Only)	N
10	Poll Program Comp. (484 Only)	N
11	Fetch Event Counter Comm.	N
12	Fetch Communications Event Log	N
13	Program (184/384,484,584)	N
14	Poll Program Complete (184/384,484,584)	N
15	Force Multiple Coils	N
16	Preset Multiple Registers	N
17	Report Slave ID	N
18	Program (884, Micro 84)	N
19	Reset Communications Link	N
20 thru 255	Reserved or Illegal	N

Figure C-1 MODBUS Function Codes

The message trailer consists of 3 bytes. The first byte of the trailer is the LRC error check character. The LRC is produced at the time of transmission from the host by adding (8-bit) the binary value of each character as it is sent. The addition is performed without wrap-around carry. When the last data character of the message has been sent the current LRC value is negated (two's compliment) and sent as the LRC (2 HEX characters). Following the LRC a carriage return and a line feed code are sent to complete the transmission. Figure C-2 shows the general format of an ASCII message exchange between a host and the Comm-Troller. All data from the MODBUS Address field thru the LRC character at the end are sent as two hex characters.

Sync Character= :	MODBUS Address	Function Code	Data As Required	LRC	Carriage Return	Line Feed
Sync Character= :	MODBUS Address	Function Code	Data As Required	LRC	Carriage Return	Line Feed

Figure C-2 MODBUS ASCII Message Exchange

1.2.2 MODBUS RTU Mode

The MODBUS RTU mode of operation is somewhat similar to the ASCII mode. In this case however, the bytes of data to be sent are not converted to printable ASCII characters. Instead, each byte is transmitted exactly with no encoding. In the RTU mode of operation the first byte of a message is defined to be the first byte received after a 3.5 character time elapse between characters. The LRC error check is replaced by a 16-bit CRC word followed by at least 3.5 character time of inactivity. Figure C-3 shows the general format of a RTU message exchange between a host and the Comm-Troller.

1.3 Message Types

MODBUS protocol communications exchanges can be divided into two types: data requests and control requests. In data requests, the host transmits a message requesting data values from the remote. The remote responds by transmitting the requested data values. These data values may be discrete (status), analog, accumulator, calculated variables, remote parameters, RTU status, analog outputs or discrete outputs. The format of the data types are as required by the host. Some variations may exist from site to site provided the host and remote are consistent in the data format (e.g. if the host expects BCD accumulator values, the remote

APPENDIX C

MODBUS PROTOCOL EMULATION

C-4
Rev. 1

>3.5 Character time	MODBUS Address	Function Code	Data As Required	CRC
------------------------	-------------------	------------------	---------------------	-----

>3.5 Character time	MODBUS Address	Function Code	Data As Required	CRC	3.5 Character time MARK
------------------------	-------------------	------------------	---------------------	-----	----------------------------

Figure C-3 Typical MODBUS RTU Message

must transmit BCD accumulator values). Note that the Comm-Troller does not do any processing on the data collected from the PLC. The PLC ladder logic must perform any data formatting that is required prior to placing the information in the data area which is read by the Comm-Troller.

Control requests are defined as any message from the host requesting the remote to change the state of a field device or to change or modify an internal condition of the remote.

1.4 MODBUS ADDRESS MAPPING

The MODBUS coil and register numbers used in the message transactions between the host and the Comm-Troller are related to the Allen-Bradley I/O ports as defined in Figure C-4.

1.4.1 Status Inputs

The current status (OFF/ON) of discrete inputs is determined by status input modules in the Allen-Bradley PLC(s). The state of the inputs is read by the MODBUS master using a "Read Input Status" command (FC=02). When this command is received the Comm-Troller will form the response from data collected from its status input cards. The mapping of MODBUS input points to Allen-Bradley inputs is one-to-one. That is, the first input of the first status input card is input 0001, the second is input 0002 and so on, up to the maximum number defined for the system.

APPENDIX C MODBUS PROTOCOL EMULATION

C-5
Rev. 1

TYPE	READ	WRITE	COIL/REGISTER #
Status Input (C-T type 0)	FC=02		1 thru 1999
Analog Input (C-T type 1)	FC=04		1 thru 128 (Analog Inputs)
			4001 thru 4128 (Frozen Analog)
Accumulator Input (C-T type 2)			3257 thru 3385
			4257 thru 4335 (Frozen Accum.)
Digital Output (C-T type 3)	FC=01	FC=05	1 thru 495 (Latched)
			501 thru 516 (Momentary)
			6001 thru 6016 (timed)
			6501 thru 7000 (Reserved)
Analog Output (C-T type 4)	FC=03	FC=06	1 thru 32 (Analog Output)
			5501 thru 5516 (Output Timers)

Figure C-4 MODBUS Address Mapping

1.4.2 Analog and Accumulator Inputs

Analog inputs are treated as Input Registers as far as the MODBUS protocol is concerned. Each input is equivalent to one "register" in MODBUS parlance and is read using the MODBUS "Read Register" command (FC=04). Analog Inputs are assigned register numbers starting at 0001 and continuing up to a maximum of 0128. Accumulators are assigned register numbers starting at 3257 and continuing up to 3385.

1.4.3 Digital Control Outputs

The Allen-Bradley digital outputs are controlled as "coils" in the MODBUS message. The current state of each output coil can be read using the "Read Coil Status" function (FC=01) and changed using the "Force Single Coil" (FC=06) command. Broadcast mode is permitted when changing the state of an output coil.

Each digital output can be controlled in three (3) different ways: Latched, Momentary and Timed. The mode of operation (latched, momentary or timed) is determined by the coil number used in the control command. Latched outputs start at coil number 0001 and continue up to a maximum of 0496. Momentary outputs start at coil number 0501 and continue up to 0516. Timed outputs start at coil number 6001 and continue up to 6016. Note that the first address in each group controls the same

physical output; the only difference is in the way in which the output from the PLC is controlled. For a latched output (0001-0496) the output is changed to the state defined by the command. For a momentary output (0501-0516) the output is first changed (if OFF then goes ON, if ON then goes OFF) and then a short time later the output is changed back to its original state. The time duration of the output is determined by a word (word 15 contact dwell time) in the configuration table headersection. For a timed output (6001-6016) the output is controlled exactly as a momentary output except that the time duration of the oputput is not fixed. Instead, the output time is determined by the current setting of a range of "pseuto" output registers (output registers 5501 thru 5516) which are discussed further in section 1.4.4 below.. Note that only the first 16 output points can be controlled in either the momentary or timed mode.; all others are latched only.

1.4.4 Setpoint Outputs

Setpoint outpus are analog outputs from the Allen-Bradley. The outputs are controlled using the MODBUS "Preset Single Register" command (FC=06). There are two types of output registers in the Comm-Troller, those that are actually connected to a corresponding Allen-Bradley PLC output register and those that are "pseudo" outputs. In the latter case, the pseudo outputs are registers maintained in the Comm-Troller which are used for Internal Control functions. At this time, the only internal registers used, define the output dwell time for the first 16 control outputs when they are operated as "timed outputs"

1.5 MODE OF OPERATION

There are two modes of operation of the MODBUS Comm-Troller. In the standard mode of operation, up to eight (8) Allen-Bradley PLCs can be connected on the data highway along with the Comm-Troller. All of the data from all of the PLCs is collected by the Comm-Troller and then merged into a single data base which will appear to the Host as a single MODBUS address. In this case, if an application has two (2) PLCs, the first with five (5) analog inputs and the second with three (3) analog inputs. The host will read the first five as registger inputs 0001 thru 0005 from MODBUS address "N". The second PLC will be read as register inputs 0006 thru 0008, also from MODBUS address "N".

In the second mode of operation, each PLC on the highway (up to 8) is assigned a unique MODBUS address. In this case, the five (5) analog inputs of PLC #1 are read by the host as registers 0001 thru 0005 from MODBUS address "N". The three (3) analog inputs of PLC #2 are read as registers 0001 thru 0003 from MODBUS address "M".

APPENDIX C

MODBUS PROTOCOL EMULATION

C-7
Rev. 1

The mode of operation and the number of inputs and outputs from each PLC is completely user selectable by filling in the configuration table as required.

1.6 MODBUS CONFIGURATION TABLE

1.6.1 MODBUS Configuration Header

BYTE	DESCRIPTION
0	RTU Number
1	Number of PLC's
2,3	Not Used
4	Baud Rate
5	Parity
6	Number of Stop Bits (1 or 2)
7,14	Not Used
15	PLC Swap Enable
16-19	Not Used
20	Gould=0/Daniel=1]
21	Mode RTU=1/ASCII=0
22	RTU Address of PLC #1
23	RTU Address of PLC #2
24	RTU Address of PLC #3
25	RTU Address of PLC #4
26	RTU Address of PLC #5
27	RTU Address of PLC #6
28	RTU Address of PLC #7
29	RTU Address of PLC #8
30-31	Momentary Contact Dwell Time
32-33	Message Resync Timeout
34-35	RTS Off Delay
36-37	Radio Key Address
38-49	Not Used

Figure C-5 Configuration Header

BYTE	DESCRIPTION
0	PLC Address
1	# Bytes per Input Status Card
2	# Input Status Cards
3,4	Start Address for INput Status Cards
5	# Bytes per Input Register Card
6	# Input Register Cards
7,8	Start Address Input Registers
9	# Bytes per Input Register Cards Gp 2
10	# Input Register Cards Gp. 2
11,12	Start Address Input Registers Gp. 2
13	# Bytes per Output Coil Card
14	# Output Coil Cards
15,16	Start Address Output Coils
17	# Bytes per Output Register
18	# Output Registers
19,20	Start Address Output Registers
21-56	Not Used

Figure C-6 PLC Data Section Config.

APPENDIX C

MODBUS PROTOCOL EMULATION

C-8
Rev. 1

Byte #0 in the configuration header is used to define the MODBUS address to which the Comm-Troller will respond when communicating with the host. This entry is an 8-bit binary number in the range of 1 to 254 (00000000 to 11111110). If this byte is zero, the Comm-Troller will assign each PLC in the cluster (up to 8) an individual MODBUS address. In this case, the MODBUS addresses are selected from a sub-table in the configuration header starting at offset 20.

Byte #1 is used to define the number of PLCs in the system. This entry is a 4 bit binary number which is right justified in the byte. The valid range for this number is from 1 to 8 (00000001 to 00001000). The Comm-Troller will use this number to determine the number of PLC Configuration blocks to read.

Bytes #2 and 3 are reserved for use as a Radio Delay Timer. The current implementation of the MODBUS protocol in the Comm-Troller ignores these bytes.

Byte #4 is used to define the baud rate which will be used while communicating with the host. This entry is a binary number which is right justified in the byte. Valid selections are: 300 baud (00000100), 600 baud (00000101), 1200 baud (00000110) , 2400 baud (00001000), 4800 baud (00001001) and 9600 baud (00001011).

Byte #5 is used to select the host communication line parity bit. Valid settings for this byte are: No Parity (00000000), Odd Parity (00000001) and Even Parity (00000010).

Byte #6 is used to select the number of Stop Bits to use when communicating with the MODBUS host. Valid selections are: 1 Stop Bit (00000001) or 2 Stop Bits (00000010)

Bytes #7 thru 14 are not recognized by the Comm-Troller for the MODBUS protocol.

Byte #15 is the PLC "SWAP" enable flag. If this byte is non-zero any failure detected by the Comm-Troller while communicating with the PLC will result in an automatic switch-over to a backup PLC. The backup PLC must have exactly the same configuration information as the primary PLC. and be connected to the same Data Highway. The backup PLC address must be address 0B_{HEX}. If the backup PLC subsequently fails the Comm-Troller will attempt to switch back to the primary unit. If this byte is zero then a switch will not be attempted.

Bytes 16, 17, 18 and 19 are not used for the MODBUS Comm-Troller.

APPENDIX C

MODBUS PROTOCOL EMULATION

C-9
Rev. 1

Byte #20 is used to specify a Gould or a Daniel mode of addressing for the Comm-Troller. In the Gould mode the first coil (coil #1) is addressed as 0000; in Daniel applications the first coil is addressed as 0001. Setting byte 20 to 0 informs the Comm-Troller that the host computer will address the points in the system using the Gould standard (zero based); if this byte is 01_H the Comm-Troller will expect the host to address the points as a Daniel host (1 based).

Byte #21 is used to select the ASCII or RTU protocols. If this byte is a zero the ASCII protocol will be used; if this byte is not zero then the RTU protocol will be used.

Byte #22 is used to specify the MODBUS address to use for PLC #1 when each PLC is to be treated as an independent device. This byte will only be used if byte #0 is equal to 0.

Byte #23 is used to specify the MODBUS address to use for PLC #2 when each PLC is to be treated as an independent device.

Byte #24 is used to specify the MODBUS address to use for PLC #3 when each PLC is to be treated as an independent device.

Byte #25 is used to specify the MODBUS address to use for PLC #4 when each PLC is to be treated as an independent device.

Byte #26 is used to specify the MODBUS address to use for PLC #5 when each PLC is to be treated as an independent device.

Byte #27 is used to specify the MODBUS address to use for PLC #6 when each PLC is to be treated as an independent device.

Byte #28 is used to specify the MODBUS address to use for PLC #7 when each PLC is to be treated as an independent device.

Byte #29 is used to specify the MODBUS address to use for PLC #8 when each PLC is to be treated as an independent device.

Bytes #30 and 31 are used to specify the contact dwell time for momentary contacts. This is a 16-bit binary number where each count is equal to approximately 10 msec.

Bytes #32 and 33 are used to specify a "message resync" time out period. In normal MODBUS RTU communication the start of message character is defined to be the first character received after a 3.5 character time delay period. In some systems, the 3.5 character delay may be exceeded because of timing delays in the communications system. This is true for most satellite systems for example. This option provides a way for the user to select an alternative delay period for defining the start of a message. The time delay will be equal to 10 msec times the value stored in bytes 32 and 33 . If bytes 32 and 33 are zero then the 3.5 character time applies.

Bytes #34 and 35 are used to specify an optional delay before the Comm-Troller will remove the RTS signal at the end of a message. This forces a quiet time at the end of the message. Typical uses for this delay are in radio systems that may require some time for the last character to get all the way thru any repeater stations. The time used will be 10 msec times the number stored in bytes 34 and 35.

Bytes #36 and 37 are used to define an optional address in the PLC (in the same file where the configuration table is located) that will be controlled by the Comm-Troller. The least significant bit in the address specified will be set on at the beginning of any response and to OFF at the end of the response in the same way that the RTS line is used on the communication port. This will allow a PLC output to be used to control a radio transmitter or other devices that may be required.

Bytes #38 thru 49 are not used for the MODBUS Comm-Troller.

1.6.2 PLC Data Configuration for MODBUS Protocol

The PLC Data Configuration section(s) are each 57 bytes long. There is one section for each PLC connected to the Comm-Troller. The number of PLCs and thus the number of configuration sections to read is defined by byte #1 in the header section of the configuration table.

Byte #0 is used to define the HEX address of the PLC on the Data Highway from which the data is to be collected.

Byte #1 is used to define the number of bytes of data for each input status card. Normally it will be set to 2 because each input card in an Allen-Bradley provides 16 bits of status information. In special applications however, PLC ladder logic could be used to form "cards" of any width.

APPENDIX C

MODBUS PROTOCOL EMULATION

C-11
Rev. 1

Byte #2 is used to define the number of input status cards associated with this PLC. A total of 256 bytes of input status (2048 points) can be defined per Comm-Troller.

Bytes #3 and 4 define the starting address (hex byte address) in the PLC for the input status data.

Bytes #5, 6, 7 and 8 are used in a similar fashion to define the input registers for the PLC. A maximum of 256 bytes of input register data (128 registers) can be defined per Comm-Troller.

Bytes #9, 10, 11 and 12 are used to define a second group of input status registers. A total of 128 bytes of additional input register data can be defined per Comm-Troller.

Bytes 13, 14, 15 and 16 are used to define output coil points. A total of 256 bytes of output coil data (2048 points) can be defined per Comm-Troller

Bytes #17, 18, 19 and 20 are used to define output registers. A total of 1280 bytes of output registers can be defined per Comm-Troller.

APPENDIX C MODBUS PROTOCOL EMULATION

C-12
Rev. 1

Bytes #21 thru 56 are not used in the MODBUS Comm-Troller. Set all bytes to zero.

1.7 JUMPER SELECTIONS FOR MODBUS

JUMPER	POSITION	JUMPER	POSITION
J2	1-2	J10	NOT USED
J3	NOT USED	J11	1-2
J4	NOT USED	J12	1-2
J5	NOT USED	J13	NOT USED
J6	1-2	J14	NOT USED
J7	1-2	J15	1-2
J8	NOT USED	J16	NOT USED
J9	NOT USED	J17	NOT USED

MODBUS Protocol Communication is on Port P1 (top port), Allen-Bradley Communication is on Port P2 (center port)

U13 = #127-007-8

U23 = #127-006-8

Figure C-7 Jumper Option Selections

PROTOCOL

The Comm-Troller jumper selections and EPROM part numbers for MODBUS protocol operation is detailed in the following figure.

Protocol	MODBUS (single RTU Address =01)
PLC Type	PLC-5/15
Comm. Data	Leased Line, 1200 baud, 1 stop, Even Parity, ASCII Mode
Num. of PLCs	One
Num. of Status	144
Num. of Analogs	5
Num. of Accums	6
Num. of Controls	112
Num. of Setpoints	6
Desired location of configuration table at word 0000 ₁₀	
Desired starting location of data at word 200 ₁₀	
Desired location for Config. Table address pointer 128 ₁₀	

Figure C-8 Example System Info.

1.8 EXAMPLE CONFIGURATION FILE

Figure C-8 details the system information that might be used to set up a typical application. This information is used to develop the configuration table information shown on the following page.

1.8.1 Comm-Troller Switch Settings

The location of the word which points to the start of the configuration table must be specified by setting the three (3) address selection switches on the Comm-Troller. For this example the switch selections are:

Pointer Address= 128₁₀ (decimal word address)

= 256₁₀ (decimal byte address)

= 0100_H (hex byte address)

PLC WORD	VALUE (HEX)	PLC WORD	VALUE (HEX)	
128	0000	025	0A02	Set Comm-Troller switches to 010 (least significant 0 is implied)
000	0101	026	0901	
001	0000	027	9002	
002	0602	028	0501	
003	0100	029	A202	1.8.2 Example Table Entries
004-014	0000	030	0601	
015	00C8	031	AC02	
016-24	0000	032	0701	
		033	B802	
		034	0601	
		035	C600	
		036-53	0000	
		054	00XX	

Figure C-9 Example
Table Entries