

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 protocol is an asynchronous byte oriented protocol designed to connect directly to modern 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, in this case the Comm-Master. 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 RTU address. This is the hardware unit number assigned to each remote. Each remote on each

APPENDIX A

Comm-Master MODBUS Protocol Emulation

A-2
Rev. 1

communication line must have a unique address. Valid addresses are 1-255 with 0 reserved as the broadcast address. The third byte of the header is the function code. This function code may range from 0 to 255. Figure A-1 details the MODBUS function codes and identifies those that are currently supported by the Comm-Master.

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

Figure A-1 MODBUS Function Codes

The message trailer consists of 4 bytes. The first two bytes of the trailer are the LRC error check. 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 carriage return and line feed codes are sent to complete the transmission. Figure A-2 shows the general format of an ASCII message exchange between a host and the Comm-Master.

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

Figure A-2 Comm-Master/RTU 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 A-3 shows the general format of a RTU message exchange between a Comm-Master and an RTU.

1.3 Message Types

MODBUS protocol communications exchanges can be divided into two types: data requests and control requests. In data requests (poll requests), the Comm-Master 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

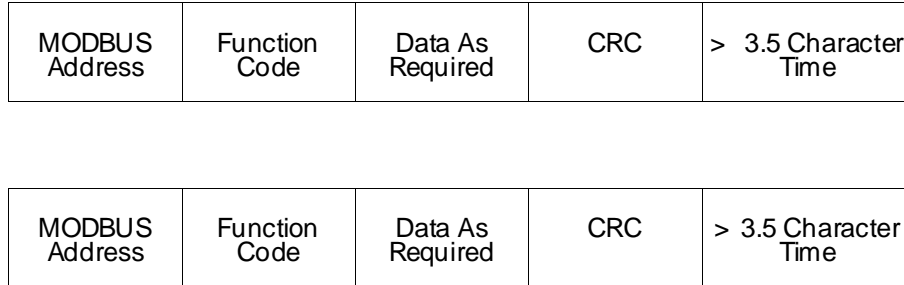


Figure A-3 Typical MODBUS RTU Message

format of the data must be as required by the master PLC. Note that the Comm-Master does not do any processing on the data collected from the remote. The PLC ladder logic must perform any data formatting that is required prior to using the data that is transferred by the Comm-Master.

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

1.4 COMM-MASTER MODBUS CONFIGURATION TABLE

The following paragraphs detail the organization of the configuration table for a Comm-Troller with MODBUS communication protocol installed on the SCADA side.

1.4.1 Comm-Master MODBUS Configuration Header

Word offset 0 is used for 2 functions: Byte # 0 is used to define the Allen-Bradley Data Highway address of the interface module that is connected to the Comm-Master. This address is typically 118 but may be assigned to other values depending on the final system configuration. The address of the data highway interface module is used as the file address when reading or writing data to a PLC-5 system. The interface module can be assigned any address from 1 through 778; Byte # 1 is used to define the number of RTU Polling Tables that are defined in the system. The Comm-Master will use this number to determine the number of Polling Table Entries to read.

Word offset 1 is used for a Radio Turn-On Delay Timer. This is the time that the Comm-Master will delay (hold-off) sending data after raising the Request To Send line (RTS). The delay time will be 10ms times the number stored in word 1.

APPENDIX A

Comm-Master MODBUS Protocol Emulation

A-5
Rev. 1

Word	Byte Numbers	Function
0	00,01	Comm-Master Address; Number of Polling Tables
1	02,03	Radio turn-on Delay (x 10 msec)
2	04,05	Radio turnoff Delay (x 10 msec)
3	06,07	RTS/CTS Delay (x 10 msec-starts after Radio turn-on delay)
4	08,09	Remote Baud Rate; # Data Bits
5	10,11	Remote Parity; # Stop Bits
6	12,13	Reserved-set to 0000H
7	14,15	Reserved-set to 0000H
8	16,17	Reserved-set to 00H; RTU Enable (ASCII= 00, RTU= 01)
9	18,19	Daniel Enable (Gould= 00, Daniel= 01); Reserved set to 00H
10	20,21	Radio Key Address
11	22,23	Poll Timer Multiplier Factor
12	24,25	Aux. Port Baud; Aux. Port # Data Bits
13	26,27	Aux. Port Parity; Aux. Port # Stop Bits
14	28,29	Aux. Port RTS ON Delay (X10ms per count)
15	30,31	Aux. Port RTS OFF Delay (X10ms per count)
16-19	24-39	Reserved-set to 0000H

Figure A-4 Comm-Master Configuration Header

Word offset 2 is used for a Radio Turn-Off Delay Timer. This is the time that the Comm-Master will hold the line quiescent after transmitting the last byte of data. This delay is sometimes required when using the Comm-Master with some types of radio systems in order to insure the proper reception at the remote end. The delay time will be 10ms times the number stored in word 2.

Word offset 3 is used for a RTS/CTS Delay timer. This is the time that the Comm-Master will delay (hold-off) sending data after raising the Request To Send line (RTS). The delay time will be 10ms times the number stored in word 3.

Word offset 4 is used for two functions. Byte # 0 is used to select the SCADA port Baud Rate. Valid settings for this byte are: 04_H= 300, 05_H= 600, 06_H= 1200, 08_H= 2400, 09_H= 4800, 0A_H= 7200 and 0B_H=9600 . Byte 1 is used to select the SCADA Port Number of data Bits option. Valid selections are: 07_H and 08_H, corresponding to seven and eight data bits respectively.

Word offset 5 is used for two options. Byte 0 is used to select the SCADA Port Parity option and byte 1 is used to select the number of stop bits to use. Valid selections for byte 0 are 00_H= no parity, 01_H= odd parity and 02_H= even parity. Valid selections for byte 1 are 01_H and 02_H, corresponding to one or 2 stop bits.

Word offsets 6 and 7 are reserved for future use. Set to 0000_H.

Word offset 8 is used for two functions. Byte 0 is reserved for future use. Byte 1 is used to select the type of communication protocol on the SCADA communication bus. Setting the low order byte to 00_H will cause the Comm-Master to communicate with the RTUs using MODBUS ASCII protocol. Setting the low order byte to non-zero will cause the Comm-Master to use MODBUS RTU protocol when communicating with the remotes.

Word offset 9 is used for two functions. Byte 0 is used to select between the Gould and Daniel modes of addressing. If byte 0 is set to 00_H then standard MODBUS addressing is used; if byte 0 is set to a non-zero value then the Daniel method of addressing is used. Byte 1 is reserved for future use.

Word offset 10 is used to define a "radio key address". The radio key address is an address in the master PLC which will be written to when the Comm-Master has data to send on its SCADA communications port. The address is entered in decimal notation. In some applications it may be necessary to switch on or "key" a radio transmitter for subsequent transmission of data. A PLC relay output module could be used for this function. If a radio key address is defined (word is non zero) then the contents of this word are interpreted as a radio key address. The Comm-Master will set bit 0 ON whenever it wishes to transmit data. The Comm-Master will clear this bit when it has no more data to sent.

Word offset 11 is used to define a "poll timer multiplier factor". Each poll table entry has a field for defining the scan update frequency (how often the poll will be issued). This time is specified in 10ms increments. In order to allow longer scan update times, the 10ms basic timer value is multiplied by the value contained in word 11. For example, if word 11 is set to 100 then the scan update frequency will be set in 1 second increments (10ms X 100 = 1sec.)

Word	Byte Numbers	Function
0	00,01	00H; MODBUS Function Code
1	02,03	Data Point Count (words)
2	04,05	00H; MODBUS Address
3	06,07	Reserved-Set to 0000H
4	08,09	Reserved-Set to 0000H
5	10,11	Data Address (High, low)
6	12,13	Destination PLC Type; Highway Address
7	14,15	Destination PLC L.P.; File Type
8	16,17	Destination PLC File Number
9	18,19	Destination PLC Starting File Element
10	20,21	Scan Update Frequency (x 10 msec)
11	22,23	Scan Error Timeout (x 10 msec)
12-15	24-31	Reserved
16	32,33	Error PLC Type; Highway Address
17	34,35	Error PLC L.P.; File Type
18	36,37	Error PLC File Number
19	38,39	Error PLC File Element

Figure A-5 Comm-Master Polling Table Entry

Word offset 12 is used for two functions. Byte #0 is used to select the Auxiliary (slave) port Baud Rate. Valid settings for this byte are: 0BH= 110 baud, 0FH= 150 baud, 1EH= 300 baud 78H= 1200 baud or F0H= 2400 baud. Byte 1 is used to select the Auxiliary Port Number of data Bits option. Valid selections are: 07H and 08H, corresponding to seven and eight data bits respectively.

Word offset 13 is used for two options. Byte 0 is used to select the Auxiliary Port Parity option and byte 1 is used to select the number of stop bits to use. Valid selections for byte 0 are 00H= no parity, 01H= odd parity and 02H= even parity. Valid selections for byte 1 are 01H and 02H, corresponding to one or 2 stop bits.

Word offset 14 is used to specify an RTS ON delay for the Auxiliary port (slave side) The delay will be 10ms times the value set in word 14

Word offset 15 is used to specify an RTS OFF delay for the Auxiliary port. The delay will be 10ms times the value set in word 15.

Word offsets 16 through 19 are reserved for future use. Set to zero.

1.4.2 Polling Table Entry for MODBUS Protocol

The Polling tables start immediately following the end of the configuration table header section. The polling tables are contiguous, one immediately following the other. Each Polling table is 20 words long. There is a polling table for each poll message that the Comm-Master is required to send. The number of polling tables to read is specified in the Configuration header word 0 byte 1 entry as described above.

Word offset 0 is used to specify the MODBUS function code to use in the poll message. Byte 0 (high byte) is set to 00H. Byte 1 is used to store the MODBUS function code that will be sent to the RTU. Valid function codes are: 01H-Read Coil Status, 02H-Read Input Status, 03H-Read Holding Register or 04H-Read Input Register

Word offset 1 is used to store the data point count (amount of data to be returned). All 16 bits can be used to specify the data point count. Byte 0 is the high order byte; byte 1 is the low order byte.

Word offset 2 is used to specify the MODBUS address which will be used in the poll message. Byte 0 is set to 00H; byte 1 is the MODBUS address.

Word offsets 3 and 4 are not used. Set to 0000H.

Word offset 5 is used to specify the data source starting address. Byte 0 is the hi order byte, byte 1 is the low order byte.

Word offsets 6 through 9 are used to specify the data destination PLC type, Data Highway Address, Logical Processor, File Type, File Number and Element. The Destination PLC is the location that the Comm-Master will use to store the data returned from an RTU poll. The first word of the address field is used to define the PLC type and data highway address. The second word is used to define the Logical Processor (PLC5/250 only) in byte 0 and the file type in byte 1. Use the hexadecimal equivalent of the ASCII logical processor number and the file type. For example, if the file to be used is an integer file (file type N) then enter a 4EH in byte 1. If the destination PLC is a PLC-2 then these fields are not used for addressing. Set this word to 0000H. The next word is used to specify the file number. Enter the hexadecimal equivalent of the file number. If the destination file is to be N10 then enter a hex 0A in this word. The file number word is not used for PLC-2 addressing. The last word is used to specify the file element that marks the start of the data to be returned. Enter the hexadecimal equivalent of the

Word	PLC2	PLC5	PLC5/250
0	02; Address	05; Address	FA;Address
1	00;00	00; File Type	L.P.; File Type
2	00; 00	File Number	File Number
3	Memory Address	Element	Element

Figure A-6 PLC Address Fields

address.

Word offset 10 is used to specify the interval between polls. Polls will be issued by the Comm-Master at the rate specified by the contents of this word. The polling interval can be specified in 10 ms increments. For example, an entry of 200 (decimal) would result in the Comm-Master polling for the data specified in this table entry once every 2 seconds (200 X 10ms per count = 2000 ms = 2 sec). Note that the timer increment is multiplied by the number stored in word 11 of the header in order to achieve longer polling intervals.

Word offset 11 is used to specify the message time-out time. The message time out will be set to the number stored in this word times 10ms.

Word offset 12 is used to specify the port to use for the MODBUS poll. Setting word 12 to 0 will direct the poll to connector P1 (top connector). Future Comm-Master modules will support MODBUS messages from the bottom port. Set word 12 to 1 to select the bottom port.

Word offsets 13 through 15 are reserved for future use. Set to 0000H.

Word offsets 16 through 19 are used to specify a Poll Message Error Address. This address will be updated by the Comm-Master at the conclusion of the poll request if an error occurs. The poll request is ended whenever either the RTU responds with the requested data or an error occurs.

1.4.3 COMMAND MESSAGE INSTRUCTION

Control commands are sent from the Comm-Master to a MODBUS device using standard ladder logic MSG instructions. The MSG instruction must be a PLC2 Unprotected WRITE command addressed to the Comm-Master (the data highway address of the RS-232 interface module that is connected to the Comm-Master). The processor type must be set to PLC-2 and the Local/Remote mode set to LOCAL. The destination data table address is not used and can be set to any value. The MSG instruction references a data table address and length. The contents of the data table referenced by the MSG instruction will be sent to the Comm-Master. The Comm-Master interprets this data to form the actual command sent to the MODBUS device. The following figure details the contents of the data block for a command MSG instruction.

Word	Byte Numbers	Function
0	00,01	Command Message Time-out (x10msec)
1	02,03	Linked Poll Number; Linked Poll Delay
2	04,05	Port Select 0= top port, 1= bottom port
3	06,07	Reserved-set to 0000H
4	08,09	Reserved-set to 0000H
5	10,11	Reserved-set to 00H; MODBUS Address
6	12,13	Reserved-set to 0000H
7	14,15	Reserved-set to 0000H
8	16,17	Starting Register/Coil Number
9-n	18-	Data for command

Figure A-7 Command Message Data

Word offset 0 is used to specify the time out value to be used for the command. The time out value is 10msec times the value stored in word 0.

Word 1 is used to optionally specify a "linked poll message". A linked poll message is a poll that is forced after the command is issued. This may be used for example to immediately read back a status line to confirm the control action specified in the control command did indeed occur. Byte 0 is used to specify the linked poll number. If no linked poll message is required set byte 0 to 00H. Byte 1 is used to specify an optional delay time. The delay time is specified in 10 msec increments. The delay time is altered by the delay timer multiplier factor stored in the header. If no delay is required set the delay time byte to 00H.

Words 2 is used to specify the port to use for the command. setting word 2 to 0 will instruct the Comm-Master to send the control out port 1 (the top port). Setting this word to 1 will send the command out the bottom port.

Word 3 is reserved for future use. Set to 000H.

Word 4 is used to specify the MODBUS command in Byte 1. The Comm-Master does not allow input commands to be built using the MSG instruction.

Word 5 is used to specify the MODBUS address that will be used in the command message.

Words 6 and 7 are reserved. Set to 0000H.

Word 8 is used to specify the starting data address that will be used in the command message.

Words 9 through N are used to contain the actual data that is to be sent as part of the command.

1.5 JUMPER SELECTIONS FOR MODBUS PROTOCOL

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

JUMPER	POSITION	JUMPER	POSITION	MODBUS Protocol Communication is
J2	1-2	J10	NOT USED	on Port P1 (top port), Allen-Bradley
J3	NOT USED	J11	1-2	Communication is on Port P2 (center
J4	NOT USED	J12	1-2	port)
J5	NOT USED	J13	NOT USED	U13 = # 166-002-X
J6	1-2	J14	NOT USED	U23 = # 166-001-X
J7	1-2	J15	1-2	
J8	NOT USED	J16	NOT USED	

Figure A-8 Jumper Settings

COMM-MASTER CONFIGURATION HEADER WORKSHEET FOR MODBUS PROTOCOL

WORD	BYTE	ADDRESS	BYTE0	BYTE1	DESCRIPTION
00	00,01				Comm-Master address; number of Polling tables
01	02,03				Radio turn-on delay (x 10ms)
02	04,05				Radio turn-off delay (x 10ms)
03	06,07				RTS/CTS Delay (x 10ms)
04	08,09				Remote baud rate; # data bits
05	10,11				Remote parity; stop bits
06	12,13		00	00	Reserved
07	14,15		00	00	Reserved
08	16,17		00		Reserved; MODBUS ASCII= 0, RTU= 1
09	18,19			00	Gould= 0, Daniel= 1; Reserved
10	20,21				Radiokey Address
11	22,23				Poll Timer Multiplier Factor
12	24,25		00	00	Aux. Baud; Aux. # data bits
13	26,27		00	00	Aux. parity; Aux. # stop bits
14	28,29		00	00	Aux. RTS ON Delay (X10ms)
15	30,31		00	00	Aux. RTS OFF Delay (X10ms)
16	32,33		00	00	Spare
17	34,35		00	00	Spare
18	36,37		00	00	Spare
19	38,39		00	00	Spare

COMM-MASTER POLLING TABLE WORKSHEET FOR MODBUS PROTOCOL

WORD	BYTE	ADDRESS	BYTE0	BYTE1	DESCRIPTION
00	00,01		00		Reserved; MODBUS Function Code
01	02,03				Data point count (words)
02	04,05		00		Data Source Address - Reserved; Address
03	06,07		00	00	Reserved
04	08,09		00	00	Reserved
05	10,11				Starting Register or Coil
06	12,13				Data Destination Address - PLC Type; Address
07	14,15				L.P.; File Type
08	16,17				File Number
09	18,19				Starting Element
10	20,21				Poll Update Frequency (x 10 ms)
11	22,23				Poll Timeout (x 10ms)
12	24,25		00		Port Select (0= P1, 1= P3)
13	26,27		00	00	Spare
14	28,29		00	00	Spare
15	30,31		00	00	Spare
16	32,33				Error Address -PLC Type; Address
17	34,35				L.P.; File Type
18	36,37				File Number
19	38,39				Starting Element

POLL TABLE

WORD	BYTE	ADDRESS	BYTE0	BYTE1	DESCRIPTION
00	00,01		00		Reserved; MODBUS Function Code
01	02,03				Data point count (words)
02	04,05		00		Data Source Address - Reserved; Address
03	06,07		00	00	Reserved
04	08,09		00	00	Reserved
05	10,11				Starting Register/Coil
06	12,13				Data Destination Address - PLC Type; Address
07	14,15				L.P.; File Type
08	16,17				File Number
09	18,19				Starting Element
10	20,21				Poll Update Frequency (x 10 ms)
11	22,23				Poll Timeout (x 10ms)
12	24,25		00		Port Select (0= P1, 1= P3)
13	26,27		00	00	Spare
14	28,29		00	00	Spare
15	30,31		00	00	Spare
16	32,33				Error Address -PLC Type; Address
17	34,35				L.P.; File Type
18	36,37				File Number
19	38,39				Starting Element

POLL TABLE

COMM-MASTER COMMAND WORKSHEET FOR MODBUS PROTOCOL

WORD	BYTE	ADDRESS	BYTE0	BYTE1	DESCRIPTION
00	00,01				Message time out (x 10ms)
01	02,03				Linked Poll # ; Linked Poll delay (x 10ms)
02	04,05		00		Port Select (0= P1, 1= P3)
03	06,07		00	00	Reserved
04	08,09		00		Reserved; MODBUS Function Code
05	10,11		00		Destination Address- Reserved; Address
06	12,13		00	00	Reserved
07	14,15		00	00	Reserved
08	16,17				Starting Register/Coil
09	18,19				Start of data

COMMAND

WORD	BYTE	ADDRESS	BYTE0	BYTE1	DESCRIPTION
00	00,01				Message time out (x 10ms)
01	02,03				Linked Poll # ; Linked Poll delay (x 10ms)
02	04,05		00		Port Select (0= P1,1= P3)
03	06,07		00	00	Reserved
04	08,09		00		Reserved; MODBUS Function Code
05	10,11		00		Destination Address- Reserved; Address
06	12,13		00	00	Reserved
07	14,15		00	00	Reserved
08	16,17				Starting Register/Coil
09	18,19				Start of data

COMMAND

WORD	BYTE	ADDRESS	BYTE0	BYTE1	DESCRIPTION
00	00,01				Message time out (x 10ms)
01	02,03				Linked Poll # ; Linked Poll delay (x 10ms)
02	04,05		00		Port Select (0= P1, 1= P3)
03	06,07		00	00	Reserved
04	08,09		00		Reserved; MODBUS Function Code
05	10,11		00		Destination Address- Reserved; Address
06	12,13		00	00	Reserved
07	14,15		00	00	Reserved
08	16,17				Starting Register/Coil
09	18,19				Start of data

COMMAND