COMMUNICATION MODBUS PROTOCOL

PR121

CE201
CONTO D2

20/10/2016

Contents

Rev	DESCRIPTION	Date	Sw
B	Formal revision	10/05/2016	➢ 1.80

1.0 ABSTRACT

Physical level

The electrical communication line complies with the EIA-RS485 standard in half-duplex modality.
In this case, as only two wires are used, only one instrument at a time can engage the line; this means that there must be a master which polls the slave instruments so the demand and the request are alternated.

On the same line only 32 instruments can be attached (master included). In order to increase the number of the slave instrument, the necessary repeaters must be used.

The communication parameters are :

Baud rate	: programmable (device dependant)
bit n.	: 8
stop bit	: 1
parity	: programmable (device dependant)

Data link level

The data are transmitted in a packet form (message) and are checked by a U_WORD (CRC).
See the description of the data packet in the next paragraphs for more details.

Application level

The communication protocol used is MODBUS / JBUS compatible.
Up to 255 different instruments can be managed by the protocol.
There are no limitations to the number of possible retries done by the master.
A delay between the response from the slave and the next command could be necessary and it is specified for each device (timing).

2.0 DATA MESSAGE DESCRIPTION

The generic data message is composed as following :

Device address	Functional code	Data	CRC word

Two answers are possible :

Answer containing data

Device address	Functional code	Data	CRC word

Error answer

Device address	Functional code + 0x80	Error code	CRC word

2.1 Parameters description

Device address : device identification number in the network.
It must be the same for the demand and the answer.
Format : 1 BYTE from 0 to 0xff
0 is for broadcast messages with no answer

Functional code : command code
Used functional code :
Format : 1 BYTE
0x03 : reading of consecutive words
0x10 : writing of consecutive words

Data : they can be
- the address of the required words (in the demand)
- the data (in the answer)

CRC word : it is the result of the calculation done on all the bytes in the message

2.2 Data format

The following types of format are used for the data values :

* U_WORD	: one WORD	- unsigned
* S_WORD	: one WORD	- signed
* UD_WORD	: two WORDS	- unsigned
* SD_WORD	: two WORDS	- signed

If the required data is in a D_WORD format, 2 WORDS are transmitted and the MSW comes before the LSW

MSB	LSB	MSB	LSB
Most Significant WORD		Least Significant WORD	

Example : 1000 = 0x 03 e8 or
0x 00 00 03 e8 (if UD_WORD)

MSB	LSB	MSB	LSB
0x00	0x00	0x03	0xe8

2.3 Description of CRC calculation

The following is an example of the CRC calculation in C language.

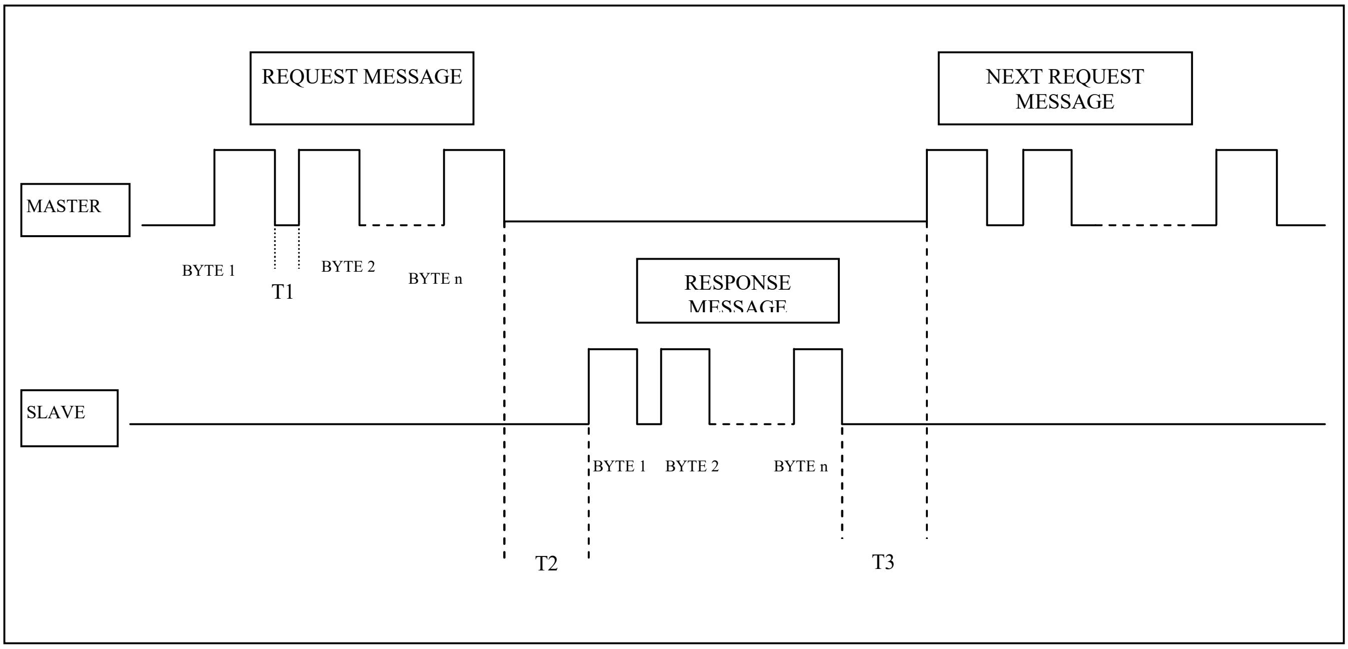
```
unsigned int calc_crc (char *ptbuf, unsigned int num)
/*    ****************************************************************
 *    Descrizione : calculates a data buffer CRC WORD
 *    Input       :       ptbuf = pointer to the first byte of the buffer
 *                 num   = number of bytes
 *    Output      : //
 *    Return      :
**    ***************************************************************/
 {
 unsigned int crc16;
 unsigned int temp;
 unsigned char c, flag;


 crc16 = 0xffff;                              /* init the CRC WORD */
 for (num; num>0; num--) {
       temp = (unsigned int) *ptbuf;          /* temp has the first byte */
       temp &= 0x00ff;                        /* mask the MSB */
        crc16 = crc16 ^ temp;                 /* crc16 XOR with temp */
       for (c=0; c<8; c++) {
             flag = crc16 & 0x01;             /* LSBit di crc16 is mantained */
             crc16 = crc16 >> 1;              /* Lsbit di crc16 is lost */
             if (flag != 0)
                  crc16 = crc16 ^ 0x0a001;    /* crc16 XOR with 0x0a001 */
       }
       ptbuf++;                               /* pointer to the next byte */
 }

 crc16 = (crc16 >> 8) | (crc16 << 8);         /* LSB is exchanged with MSB */

 return (crc16);

} /* calc_crc */
```

2.4 Error management

If the received message is incorrect (CRC16 is wrong) the polled slave doesn’t answer.
If the message is correct but there are errors (wrong functional code or data) it can’t be accepted, so the slave answers with an error message.

The error codes are defined in the following part of the document.

2.5 Timing



TIME	DESCRIPTION	Min & Max VALUES
T1	**Time between characters.** If this time exceeds the max. time allowed, the message is not considered by device.	Typ. = 20 ms
T2	**Slave response time** Minimum response delay to Master request.	Min = 20 ms
T3	Time before a new message request from the Master can be issued	Min = 1 ms

3.0 COMMANDS

Code 0x03 : reading of one or more consecutive WORDS

Command format :

BYTE	BYTE	MSB LSB	MSB LSB	
Device address	Funct. Code	First WORD address	WORDS number	CRC16

Answer format (containing data) :

BYTE	BYTE	BYTE	MSB LSB	MSB LSB	
Device address	Funct. Code	BYTES number	WORD 1	WORD N.	CRC16

The BYTES number must always match the WORDS number (in the demand) * 2.

Answer format (the demand was wrong) :

BYTE	BYTE	BYTE	
Device address	Funct. Code + 0x80	Error code	CRC16

Error codes :
* 0x01 : incorrect functional code
* 0x02 : wrong first WORD address
* 0x03 : incorrect data

Code 0x10 : writing of more consecutive WORDS

Command format :

BYTE	BYTE	MSB LSB	MSB LSB	BYTE	MSB LSB	MSB LSB	
Device address	Funct. Code	First WORD address	WORDS number	BYTE numbers	Word Value		CRC16

Answer format (containing data) :

BYTE	BYTE	MSB	LSB	MSB	LSB	
Device address	Funct. Code	First WORD address		WORD N.		CRC16

The BYTES number must always match the WORDS number (in the demand) * 2.

Answer format (the demand was wrong) :

BYTE	BYTE	BYTE	
Device address	Funct. Code + 0x80	Error code	CRC16

Error codes :
* 0x01 : incorrect functional code
* 0x02 : wrong first WORD address
* 0x03 : incorrect data

4.0 VARIABLES

Address	**Length**	**Description**	**Unit**
0x2000	UD_WORD	Voltage	mV
0x2002	UD_WORD	Current	mA
0x2004	UD_WORD	Active power	0.01 W (100.23 => 10023)
0x2006	U_WORD	Sign of active power	0 : pos 1 : neg
0x2007	U_WORD	Power factor	1/100
0x2008	U_WORD	Sector of power factor (cap or ind)	0 : PF = 0 or 1 1 : ind 2 : cap
0x2009	U_WORD	Frequency	0.1 Hz (50.0 => 500)
0x200a	UD_WORD	Positive active energy	0.1 kWh (100.2 => 1002)
0x200c	UD_WORD	Positive partial active energy	0.1 kWh (100.2 => 1002)
0x200e	UD_WORD	Operating time counter	sec.
0x0c8	U_WORD	Reset - bit to bit defined	(1)
0x300	U_WORD	Device identifier	0x13

(1) ---

WRITABLE ONLY

0x01 : partial active energy reset
0x08 : operating time counter reset