ModBus-RTU

Description of the protocol

Version: 4.0

11. September 2018

Rawet Studio

Rawet Ltd.

Čapkova 22

678 01, Blansko

515 416 942

http://www.rawet.cz

1. Table of contents

2. Description of functions

Communication with the transmitter is on the principle of MASTER - SLAVE.

Protocol MODBUS has the following structure:

<toff> <slave address> <function> <data> <CRC> <toff>

description parts of the protocol		
part of the protocol	meaning	number of bits
<toff>	delay more than character	
<slave address>	address from the range <1 … 247>	8 bits
<function>	code number of the function	8 bits
<data>	meaning is given by the description of individual parts	N * 8 bits
<CRC>	checksum	16 bits

The command is represented by a tuple eight-bit data. If during the transmission is delay greater than time corresponding to dispatch 4 characters at a given baud rate, command receive is interrupted and decodes. First, it checks the CRC. If the converter gets incomprehensible data does not match. If the converter gets data with your address, but which contain a syntax error, responds with an error message. (see error table).

If the unit is correctly received command, it responds with the same answer as the query structure after a period longer than toff.

func.nr.	meaning	data command	data response
01_H	relay status reading	16b – number of relay	8b – number of bytes on response 8b – binary state of the relays
03_H 04_H	reading 16b of data	16b - address reading register 16b – number of reading registers	8b – number of bytes on response 2*N bytes - data from registers
06_H	write 16b of data to the memory	16b – address of write 16b – value data write	16b – address of write 16b - value data write
08_H	converter reset	0001_H $FF00_H$	0001_H $FF00_H$
11_H	Report Slave ID	nothing	8b - number of bytes on response (always 02_H) MSB – type of converter LSB – SW version

return

Functions 01_H

Functions 01_H is used for reading state of 16b relays.

The command structure is as follows:

<converter address> <01> <0018> <number of ralays reading<CRC>

Meaning of parameters	
part of the protocol	meaning
converter address	8b value from the range <1 .. 247>
register address	16b address the first reading address – always <0018_H>
number of relays readings	16b number of relays readings acceptable values are only 0001_H, 0002_H a 0004_H
CRC	checksum

Answer a properly specified command is:

<converter address> <01> <2*N> <8b binary state of the relay > <CRC>

In the event of an error in the command is coming error message (see error table) or converter does not respond at all.

example		
description	command example	response example
reading state relay 1, 2	01 01 0018 0002 $3DCC_H$	01 01 01 02 $D0F2_H$ relay2 switch on, relay 1 switch off

return

Functions 03_H a 04_H

Functions 03_H a 04_H are the same. They are used for reading value of 16b register from the specified address.

The command structure is as follows:

<converter address> <03 or 04> <register address> <number of registers> <CRC>

Meaning of parameters	
part of the protocol	meaning
converter address	8b value from the range <1 .. 247>
register address	16b address the first reading address
number of registers	16b number of consecutive read registers acceptable values are only 0001_H, 0002_H a 0004_H
CRC	checksum

Significance of converter memory is shown in the table memory.

Answer a properly specified command is:

<converter address> <03or 04> <2*N> <N*16b data values of consecutive registers > <CRC>

In the event of an error in the command is coming error message (see error table) or converter does not respond at all.

example		
description	command example	response example
Reading input value 32b	01 04 0003 0002 $81CB_H$	01 04 04 FFFF FFCD $7BC5_H$ (-0,51 °C)
Reading 2*input value 2*32b	01 04 0001 0004 $A009_H$	01 04 08 0000 0280 FFFF FFCD $A470_H$ (+6,40 a -0,51 °C)

return

3. Function 06_H

Function 06_H is used for write data value to the specified memory of the converter.

The command structure is as follows:

<converter address> <06> <register address> <data value> <CRC>

Meaning of parameters	
part of the protocol	meaning
converter address	8b value from the range <1 .. 247>
register address	16b address the first reading address
data value	16b value of data which you can write to the specified memory
CRC	checksum

Significance of converter memory is shown in the table memory.

Answer a properly specified command is:

<converter address> <06> <address of register> <16b data values> <CRC>

In the event of an error in the command is coming error message (see error table) or converter does not respond at all.

example		
description	command example	response example
write 16b value	01 06 1032 0C02 $A804_H$	01 06 1032 0C02 $A804_H$

Note: Values written to memory locations specifying the device configuration to take effect after a reset (see function 08h).

return

4. Function 08_H

Function 08_H will do SW reset of the converter.

The command structure is as follows:

<converter address> <08> <$0001FF00_H$> <CRC>

Meaning of parameters	
part of the protocol	meaning
converter address	8b value from the range <1 .. 247>
$0001FF00_H$	fixed constant
CRC	checksum

Answer a properly specified command is the same as command.

In the event of an error in the command is coming error message (see error table) or converter does not respond at all.

Note: The Reset command is necessary to do always when change the transmitter configuration or after the change in the configuration of communication.

return

5. Function 11_H

Function 11_H serves to identify the transmitter and its included software.

The command structure is as follows:

<converter address> <11> <CRC>

Meaning of parameters	
part of the protocol	meaning
converter address	8b value from the range <1 .. 247>
CRC	checksum

Answer a properly specified command is:

<converter address> <11><number><type><SW> <CRC>

Meaning of parameters in the answer	
part of the protocol	meaning
converter address	8b value from the range <1 .. 247>
register address	16b address the first reading address
number	8b number of bytes on answer-are only 02_H
type	70_H - PPL112 $6E_H$ - PPL110 64_H - PPL100 $D2_H$ - PXL210 $D4_H$ - PXL212 $3A_H$ - PXL310 $3C_H$ - PXL312 24_H - R24
SW	number of SW
CRC	checksum

In the event of an error in the command is coming error message (see error table) or converter does not respond at all.

example		
description	command example	response example
identification R24 version SW 4	01 11 C0 $2C_H$	01 11 02 2404 $A7FF_H$

return

6. Error table

If an error occurs after the function call will be in error response the number of function increased about 80H. In the data, followed by the error number.:

<address> <function +80_H> <error number> <CRC>

error number	
01_H	unknown function
02_H	error in the number of registers
03_H	error in other data
04_H	Input is out of range (disconnected, short-circuit)

Example of an error message with the address 02_H converter with input out of range when you call the function 03_H is as follows:

$(02\ 83\ 04\ B0\ F3)_H$

7. Address of input registers

description of meaning input registers			
address	length	value	availability
0001H	16b	2*16b input value (long integer)	only read
0002H			
0011H		16b input value (integer)	
0064H	32b	32b input value (long integer)	
0066H		32b input value (float IEEE-754)	

return

8. EEPROM map

To write values and addresses of the memory is used for 16-bit value written in hexadecimal.

description of meaning of addresses in the address			
memory	value		availability
1000_H to 1029_H	linearization data		read/write
1029_H	number of decimal places and type of input quantity (see table 3)		
$102A_H$	configuration word (see table 1)		
$102B_H$	correction of input 1 *)		
$102D_H$	MSB month of calibration LSB year of calibration		
1032_H	MSB communication parameters (see table 2) LSB converter address		
1034_H a 1035_H	32b serial number		only read
1100_H	number of decimal places in the view brightness and display interval (see table 5)		read/write
1101_H to 1104_H	relay 1	24b. IEEE-754**) limits and mode (see table 4)	
1105_H to 1108_H	relay 2		
1109_H to $110C_H$	relay 3		
$110D_H$ to 1110_H	relay 4		
1111_H to 1114_H			
1115_H to 1118_H			
1119_H to $111C_H$			
$111D_H$ to $111E_H$			

*) The correction value input is 16-bit hexadecimal number in supplemental form.
We can express both positive and negative shift of a given number of digits.
Shift of +1 digit number is expressed as 0x0001,
shift by -1 digit number then 0xFFFF
**) The IEEE-754 24b value is created as 32b IEEE-754, with the lowest 8b of the mantissa omitted.
Ex. The converted value of 100 is in the 32b IEEE-754 0x42c80000 after the truncation to 24b IEEE-754 is 0x42cb800
***) The conversion of temperature sensors is 1: 1 and can not be changed. For others we can choose. From the displayed value, both the relay limits and the output range are set.

return

9. Table 1 - Meaning of bits in the configuration word ($102A_H$)

Bit	meaning	description
16 (MSB)	unmeaning	0
15		
14		
13		
12		
11		
10		
9		
8	analog output	0 – yes, 1 - no
7	response to the overflow	0 - error message 1 – value about 6% out of range
6	unmeaning	0
5	filter	0 - filter OFF 1 - filter ON
4	output 0..20mA	1 - ON
3	swap order of the output 32b	0 - 16b MSB then 16b LSB 1 - 16b LSB then 16b MSB
2	compensation	0 - 3W or cold junction compensation 1 - 2W or without cold junction compensation
1 (LSB)	resolution of the input	0 - 15 bits 1 - 14 bits

*) is valid if the register 1120H is a nonzero value if is 0 in this register there is 0..10V output.

return

10. Table 2 - Meaning of bits in the communication word

bit	meaning	description
16 (MSB)	unmeaning	0
15		
14		
13	baud rate [Bd]	00 - 19200Bd 01 - 9600Bd 10 - 4800Bd 11 - 2400Bd
12		
11	parameters (number of data bits parity number of stop bits)	1xx - 8N1 **) 000 - 8E1 001 - 8O1 01x - 8N2
10		
9		
8	device address (express in binary code)	number of range <1 .. 247>
7		
6		
5		
4		
3		
2		
1		

**) x - regardless of the value of the bit.

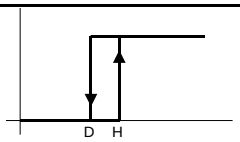
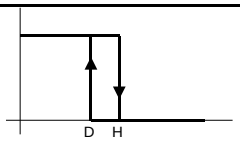
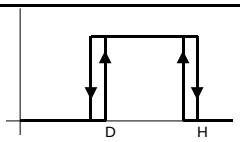
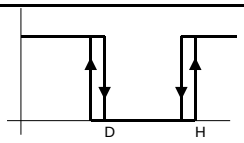
return

11. Table 3 - Meaning of bits in the register 1029_H

bit	meaning	description
16 (MSB) 15	number of decimal point in the input register	11b – 3 dp 10b – 2 dp 01b – 1 dp 00b – 0 dp
14 13 12	unmeaning	
11 10 9	converter input	111 – R[kΩ] 110 – R[Ω] 101 – I[mA] 01x – U[mV] 00x – RTD[°C]
8 7 6 5 4 3 2 1 (LSB)	configuration of input circuits	it is the part of the linearization ATTENTION! never change!

return

12. Table 4 – Relay modes

Relay modes	modRD	modRH	
Switch ON	0x01	0x02	
Switch OFF	0x02	0x01	
Permanently closed	0x20	0x20	
Permanently open	0x10	0x10	
Switch ON window	0x41	0x41	
Switch OFF window	0x42	0x42	
No relay	0x80	0x80	

The relay setting is determined by two values D and H, which are stored in the IEEE754 24b format. In total, there are 4 registers. In the lower pair of 4 registers, the value D is stored, then the value H is higher. The relay mode is then stored in the lowest byte of the two registers pairs. The values D and H are always stored in the displayed units.

If one of the window modes is selected, then the same hysteresis specified in $111D_H$ and $111E_H$ in the IEEE754 32b format for all relays in window mode is the same.

The value D1 is located on adress 1102_H, and in the upper byte 1101_H in the lower byte is the mode of relay. Analogously H1 on address 1104_H and in the upper byte 1103_H and mode of relay then in lower byte.

An example can be set to the switch ON mode D = 23, H = 25.

H=25=0x41c800, mod=0x02 -> reg 0x1104=<0x41c8>, reg 0x1103=<0x0002>

D=23=0x41b800, mod=0x01 -> reg 0x1102=<0x41b8>, reg 0x1101=<0x0001>

return

13. Table 5 – Meaning of bits in the register 1100_H

bit	meaning	description
16.-15.	no	
14.-13.	number of decimal point	00– 0 decimal point 01– 1 decimal point 10– 2 decimal point 11 – 3 decimal point
12.-9.	display brightness	brightness on the interval 0x0-0xf
8.	no	
7.-1.	display period	period on the interval 0x00-0x0f (0,5s-8s)

return