Communication protocol

1 Introduction

PAS6000 communication protocol is described in detail the serial port communication reading and writing data command format and the definition of inside information to third-party developers to use.

1.1 PLC ModBus Compatibility

ModBus communication protocol allows PAS6000 and Schneider, Siemens, AB, GE, Modicon, and other well-known international brands of programmable sequence controller (PLC), RTU, SCADA systems, DCS, or third-party monitoring system compatible with the ModBus information between and the effective transmission of data. With PAS6000, to simply increase the set-based PC (or IPC) of the central communication master display software (such as: configuration king, Intouch, FIX, synall, etc.) can establish a monitoring system.

1.2 Integration of a wide range of communications

PAS6000 provides the system compatible with the Modicon ModBus communication protocol, the communication protocol is widely used as system integration standards. Compatible interface, programmable logic controllers RS-485/232C ModBus communication protocol allows information and data in the PAS6000 and Modicon programmable logic controllers (PLC), RTU, SCADA systems, DCS systems and other compatible systems ModBus communication protocol between effective deliveries.

2 ModBus Basic Rules

2.1 RS485 communication loop should be in accordance with all the master / slave mode。According to this way, data can be a master station (eg: PC) and 32 sub-stations (such as: PAS6000) pass between.

2.2 Master station to initialize and control the RS485 communication all the information passed back to the road.

2.3 Any time communication is not started from the slave station.

2.4 RS485 loop in all communications with "information frame" method to pass.

2.5 If the master station or slave station receives the frame with unknown commands, not to be responding.

"Information frame" is a data frame (each byte is a data frame) to form a string (up to 255 bytes) is sent by the message header and the encoded data constitute a standard asynchronous serial data, the communication ways compatible with the RTU communication protocol.

3 Data frame format:

For asynchronous transfer mode communications, and bytes (data frame) as the unit. In the main station and sub-stations for each data frame transmission is 11-bit serial data stream.

Data frame format:

Start bits	1 byte
Data bits	8 bytes(Low front, high in the post)
Parity	1byte：Have parity；no：No parity
Stop bit	1byte：Have parity；2 bytes：No parity

4 PAS6000 Communication protocol

When the communication command sent to the instrument, in line with the corresponding address of the device to receive communication command code, and remove the address code, read the information, if not wrong, then perform the appropriate tasks; then sent back to the sender results of the implementation. Send the information back to include the address code, function code perform the action, after the implementation of actions and error check code data (CRC). If the error does not send any information.

4.1 Message frame format

START	**ADDRESS**	**CS**	**DATA**	**CRC**	**END**
Initial structure	Address code	Function Code	Data area	Error checking	End structure
Delay (equivalent	1 byte	1 byte	N bytes	2 bytes	Delay (equivalent

to 4 bytes of the time)	8 bits	8 bits	N×8bits	16bits	to 4 bytes of the time)

4.1.1 Address code (ADDRESS)

Address code for each communication information transmitted data frames in the first frame (8), from 0 to 255. The byte address code set by the user that the sub-unit will receive the information is sent by the host. And each sub-unit has a unique address code, and the response are sent back to the beginning of their respective address code. Send the address of the host code that is sent to the sub-machine address, and sub-machine code that send the address to send the child back to the machine address.

4.1.2 Function Code (CS)

Function code is transmitted each time the information communication in the second frame data frame. ModBus communication protocol defined function code is 1 ~ 127 (01H ~ 7FH). PAS6000 use one part of the function code. As a host request, through the function code to tell what action the implementation of slave machine. As a slave machine response, the master sends the function code and function code sent by the host, like, and that slave respond to the host machine has to operate. If the child sends the function code of the highest bit is 1 (Function Key "127), then the slave machine is not responding or wrong.

The following table lists the function codes have specific meaning and operation.

MODBUS function code section

Function Code	**Definition**	**Operation**
03H	Read register	Read data from one or more register
06H	Write Single Register	A 16-bit binary number to write a single register
10H	Write Multiple Registers	A 16-bit binary number to write to multiple registers

a) 03，Read register

PAS6000 using ModBus communication protocol, the use of communications command, you can read point (to keep a register or return value input register). 03H mapping function code data area of the maintenance and input register values are 16-bit (2 bytes). This register is read from the PAS6000 is 2 bytes. Read register number, up to 125. Since some programmable controllers does not function code 03, so the function code is used to read 03 point and return values.

Slave machine response command format is the machine address, function code, data area and the CRC code. Data area of the data is 2 bytes each for a group of double-byte number, and the high byte first.

b) 06，Write Single Register

Master uses this command to save data to a single point of intelligent electricity transmitter PAS6000 memory. This feature is also used slave machine code to send information back to the master.

c) 10, Write Multiple Registers

Master uses this command to save data to PAS6000 more memory. Modbus communication protocol of the register refers to the 16-bit (ie 2 bytes), and high in the former. This intelligent power meter PAS6000 points are two bytes. With a command to save the maximum number of points depends on the slave machine. Modbus communication protocol allows for up to save 60 registers, so that smart electricity transmitter PAS6000 allows a maximum of 60 registers can be saved. PAS6000 smart electricity transmitter unit command format is the address, function code, data area and the CRC code

4.1.3 DATA Area

With the function code data area varies. Sent by the master read command (03H) information sub-frame data area and the data frame response message unit area is different, sent by the master write command (06H, 10H) information data area and the sub-frame response message frame machine data area is the same. Slave machine data area contains the implementation of any action required or collected by the slave machine needs to send information back. This information can be numbers, reference addresses and more. For example, the function code to tell slave machine read register values, the data area must contain the start address register to be read and read length (register number).

a) The function of the corresponding data area code format 03

Master Send

Data sequence	1	2

Data meaning	Start Address	Read register number
Bytes	2	2

Slave answers

Data sequence	1	2
Data meaning	The number of bytes sent back to	N data registers
Bytes	1	2×N

b) The function of the corresponding data area code format 06

Data sequence	1	2
Data meaning	Start Address	The data written to the register
Bytes	2	2

c) The function code data area corresponding to the format of 10

Data sequence	1	2	.....	N
Data meaning	Start Address	Write Register 1	.....	Write Register N
Bytes	2	2	.....	2

4.1.4 Error check code (CRC)：

Master or Slave machine check code can be used to determine whether the information received error. Sometimes, due to electronic noise or other interference during the transmission of information in the subtle changes occur, the error check code to ensure that the Master or Slave machine errors in the information transmission process does not work. This increases system security and efficiency. Error check code CRC-16 checksum with method

Two bytes error checking code, low byte first, high byte.

Note:

The format of the information frame is the same: address code, function code and error check code data area.

5 Error checking

Cyclic redundancy code (CRC) contains 2 bytes, or 16-bit binary. CRC code calculated by the sender, send a message placed in the rear. Receiver device and then re-calculate the CRC code to the information received, comparing the calculated CRC code is consistent with the received, if the two do not match, then the error.

CRC code is calculated, the first 16-bit registers are all preset. And then gradually to every 8-bit data processing. CRC code calculation making only 8 data bits, start bit and stop bits, parity bit if the words are also included parity bit, do not participate in CRC code calculation.

In calculating the CRC code, the 8-bit data and register data differences or, the results obtained, a shift to lower, with 0 fill the highest. And then check the lowest, if the lowest bit is 1, the contents of the register and the number of different preset or, if the lowest bit is 0, without XOR.

The process is repeated 8 times. 8th shift, the next 8-bit register contents then and now different, or, as the process repeated with the above 8 times. When all the data processed, the contents of the final register is the CRC code value.

6 Code CRC-16 calculation steps

a) 16-bit register is set to hexadecimal FFFF (which are all 1.) This register is called CRC register.

b) to an 8-bit data and low 16-bit CRC register, or different, the results put in the CRC register.

c) to register the contents of the right one (towards the low), with 0 to fill the highest, check the lowest bit (out of the bit).

d) If the minimum is 0: Complex Step 3 (again the shift).
If the lowest bit is 1: CRC register with the polynomial A001 (1010 0000 0000 0001) XOR.
e) Repeat steps 3 and 4, until the right 8 times, so that all of the 8-bit data were processed.
f) Repeat steps 2 through 5, the next 8-bit processing.
g) The resulting CRC is the CRC code register, low byte first, high byte.
7 For example frame format information
7.1 Function code 03
Slave address 01, start address 0032 of the three registers.
Address register data in this case is:

Address	Data(16 hex)
0032	EA60
0034	C350
0036	DB6C

Master send	Bytes	For example(16 hex)	
Slave Address	1	01	Send to slave 01
Function Code	1	03	Read register
Start Address	2	00	Start address is 0032H
		32	
Read register number	2	00	Read 3 Registers (6 bytes)
		03	
CRC Code	2	A4	The CRC code calculated by the master
		04	

Slave answer	Bytes	For example(16 hex)	
Slave Address	1	01	From slave 01
Function Code	1	03	Read register
The number of bytes read	1	06	3 Registers (6 bytes)
Register data 1	2	EA	Address the contents of 0032
		60	
Register data 2	2	C3	Address the contents of 0034
		50	
Register data 3	2	DB	Address the contents of 0036
		6C	
CRC Code	2	D1	The CRC code calculated by the slave
		3F	

7.2 Function code 06
01 slave address, save the start address 0002 of the two values. In this case, the data is saved after the end of 0002 slave address of the content within the 0002.

Master send	Bytes	For example(16 hex)	
Slave Address	1	01	Send to slave 01
Function Code	1	06	Single data (2 bytes) to preserve
Start address	2	00	Start address is 0002
		02	
Save data	2	00	Save data is 0002
		02	
CRC Code	2	A9	The CRC code calculated by the master
		CB	

Slave answer	Bytes	For example(16 hex)

Slave Address	1	01	From slave 01
Function Code	1	06	Save a single register
Start address	2	00	Start address is 0002
		02	
Save data	2	00	Save data is 0002
		02	
CRC Code	2	A9	The CRC code calculated by the slave
		CB	

7.3 Function Code 10

01 slave address, the 0064 save to address 0000. In this case, the data saved, the address is 01 PAS6000 intelligence information stored within the transmitter power：

Address	Data(16 hex)
0000	0064

Master send	**Bytes**	**For example(16 hex)**	
Slave address	1	01	Send to slave 01
Function code	1	10	Single data (2 bytes) to preserve
Start address	2	00	Start address is 0000
		00	
Save data number	2	00	Save 2 registers（4 bytes）
		02	
Bytes	1	04	
Save data 1	2	00	Data address is 0002
		64	
Save data 2	2	00	Data address is 0000
		00	
CRC code	2	B2	The CRC code calculated by the master
		70	

Slave answer	**Bytes**	**For example(16 hex)**	
Slave address	1	01	From 01 slave
Function code	1	10	Save more registers
Start address	2	00	Start address is 0000
		00	
Save data number	2	00	Save 2 registers（4 bytes）
		02	
CRC code	2	41	The CRC code calculated by the slave
		C8	

8 Error handling

When the PAS6000 smart electricity transmitter detected an error other than CRC error code to be sending information back to the master, the highest position function code is 1, that is, slave back to the function code is sent to the master the master to send the function code based add to 128. These codes indicate the following unexpected error has occurred.

The information received from the master, if any CRC error, it will be PAS6000 smart electricity transmitter ignored.

Slave error code sent back the following format (CRC codes excluded)

Address code：	1byte
Function code：	1byte(MSB is 1)

Error code：	1byte
CRC code：	2bytes

PAS6000 smart electricity transmitter to send the following error response back to command

01	Illegal function code。 Received function code PAS6000 does not support
02	Illegal data location Location of the specified data range beyond the PAS6000
03	Illegal data value Received the data sent to the host address exceeds the range of data corresponding

Appendix I：*Register map table*

Table 1 Function Code 03H data area of the map - basic data:

Basic data

No.	Address	Item	Notes
1	0000H	Ua	Voltage Phase 1
2	0002H	Uca	Voltage Line 31
3	0004H	Ia	Current Phase 1
4	0006H	Fa	
5	0008H	Pa	Active Power Phase 1
6	000AH	PFa	Power Factor Phase 1
7	000CH	Qa	Reactive Power Phase 1
8	000EH	Sa	Apparent Power Phase 1
9	0010H	Ub	Voltage Phase 2
10	0012H	Uab	Voltage Line 12
11	0014H	Ib	Current Phase 2
12	0016H	Fb	
13	0018H	Pb	Active Power Phase 2
14	001AH	PFb	Power Factor Phase 2
15	001CH	Qb	Reactive Power Phase 2
16	001EH	Sb	Apparent Power Phase 2
17	0020H	Uc	Voltage Phase 3
18	0022H	Ubc	Voltage Line 23
19	0024H	Ic	Current Phase 3
20	0026H	Fc	
21	0028H	Pc	Active Power Phase 3
22	002AH	PFc	Power Factor Phase 3
23	002CH	Qc	Reactive Power Phase 3
24	002EH	Sc	Apparent Power Phase 3
25	0030H	I0	Neutral Current
26	0032H	Uav	Average Voltage Three Phase
27	0034H	Iav	Average Current Three Phase
28	0036H	F	Frequency
29	0038H	Psum	Total Active Power
30	003AH	PFav	Total Power Factor
31	003CH	Qsum	Total Reactive Power
32	003EH	Ssum	Total Apparent Power

Table 2 Function Code 03H data area of the map – Energy:

No.	Address	Item	Notes
1	0042H	+Wh(L)	Positive active energy accumulator low word
2	0044H	+Wh(H)	Positive active energy accumulator high word
3	0046H	-Wh(L)	Negative active energy accumulated value to the low word
4	0048H	-Wh(H)	Negative active energy accumulated value to the high word
5	004AH	+Varh(L)	Positive reactive energy accumulator low word
6	004CH	+Varh(H)	Positive reactive energy accumulator high word
7	004EH	- Varh(L)	Negative reactive energy accumulator low word
8	0050H	- Varh(H)	Negative reactive energy accumulator high word

Table 3 Function Code 03H system parameters are mapped:

Address	Item	Bytes	Notes	Initial state
0300H	Local Address	2	1～247	0
0302H	Measurement system wiring	2	0 Three-phase four-wire	0
			1 One-phase two-wire	
			2 Three-phase three-wire	
			3 Three-phase three-wire balance	
			4 One-phase three-wire	
			5 Three-phase four-wire balance	
0304H				
0306H	Parity	2	0/1/2（N/O/E）	0
0308H	Baud Rate	2	0 1200	3
			1 2400	
			2 4800	
			3 9600	
			4 19200	
030AH	Voltage input range	2	0 150 V	1
			1 600V	
030CH	Power unit	2	0 WH	0
			1 10WH	
			2 100WH	
			3 KWH	
			4 10KWH	
			5 100KWH	
			6 MWH	
030EH	PT	4	1～64000	1
0312H	CT	4	1～64000	1
0316H～035FH	Manufacturers Reserved			

Table 4 Function Code 06H data area of the map:

Address	Item	Notes
0000H	Local address	0～247
0002H	Measurement system wiring	0 Three-phase four-wire
		1 One-phase two-wire
		2 Three-phase three-wire
		3 Three-phase three-wire balance
		4 One-phase three-wire
		5 Three-phase four-wire balance
0004H	Clear the maximum / minimum values	0 disable
		1 enable
0008H	Baud Rate	0 （1200）
		1 （2400）
		2 （4800）
		3 （9600）
		4 (19200(Reserved))
0016H～005FH	Manufacturers Reserved	

Tale 5 Function Code 10H data area of the map:

Item	Start address	End address	Range	Unit
PT	0000H	0003H	1～64000	1
CT	0004H	0007H	1～64000	1

Appendix II :Data transformation

All the data output from the PAS6000 responses are standardized according to certain formulas into 2 bytes Rx, energy, except for 4 bytes.

NO	Item	Formula	Range	Symbol	Notes			
1	Voltage,V	U = Rx×PT×0.01	0～65535	No	Ua	Ub	Uc	Ue0
					Uca	Uab	Ubc	Ue
2	Current,A	I =Rx×CT×0.0001	0～65535	No	Ia	Ib	Ic	Ie
3	Frequency,Hz	F=Rx×0.00106813	0～65535	No	F			
4	Power Factor,PF	PF =Rx×0.0001	-10000～10000	Yes	PFa	PFb	PFc	PFs
				+: Delay load / -: ahead of the load				
5	Active Power,W	P= Rx×PT×CT×0.4	-32768～32768	Yes	Pa	Pb	Pc	P
6	Reactive Power,Q	Q =Rx×PT×CT×0.4	-32768～32768	Yes	Qa	Qb	Qc	Q
7	Apparent Power,S	S= Rx×PT×CT×0.2	0～65535	No	Sa	Sb	Sc	S
8	Energy,Wh	Wh=Rx×K(K= Energy Unit)	$0～10^9$	No	+Wh	-Wh	+Varh	-Varh

A screenshot of output:

Tx:01 03 00 00 00 20 44 12 -----Get the basic data list
Rx:01 03 40 **57 F2** 2C 50 00 00 B6 DD 00 00 00 00 00 00 00 00 2B D6 2C 20 00 00 B6 DD 00 00 00 00 00 00 00 00 2B B5 00 00 00 00 B6 DD 00 00 00 00 00 00 00 00 00 00 3A 7D 00 00 B6 DD 00 00 00 00 00 00 00 00 00 7A 7B

（57 F2）HEX=22514, Voltage Phase 1=22514/100=225.14 Volts AC，