SPM90
MODBUS PROTOCOL
AND REGISTER LIST
V1.3

ZHUHAI PILOT TECHNOLOGY CO., LTD.

www.pmac.com.cn

CONTENTS

1. Introduction

This document describes the input and output command, information and data of the SPM90 under MODBUS communication mode. So it is convenient for the 3rd part using and developing.

1.1 Purpose of the Communication Protocol

The purpose of the SPM90 MODBUS communications protocol is to allow setup information and measured data to be efficiently transferred between a MODBUS Master Station and SPM90. It includes:

1) Allowing setting and reading all SPM90 set-up parameters from a MODBUS Master Station.

2) Allowing reading all data measured by a SPM90 and SOE (Event log).

1.2 Version of Communication Protocol

This document is proper for all versions of SPM90 meters. It will be declared, if any change happens later.

2. Detailed Description of the SPM90 Modbus Protocol

2.1. SPM90 Modbus Protocol Rules

The following rules define the protocol rules for information transfer between a MODBUS Master device and the SPM90 in a RS-485 serial communications loop.

1) All communications on the RS-485 loop conforms to a MASTER/SLAVE scheme. In this scheme, information and data is transferred between a MODBUS MASTER device and up to 32 SLAVE monitoring devices.

2) The MASTER will initiate and control all information transfer on the RS-485 communications loop.

3) Under no circumstances will a SLAVE device initiate a communications sequence.

4) All communications activity on the RS-485 loop occurs in the form of "PACKETS", a packet being simply a serial string of 8-bit bytes. The maximum number of bytes contained within one packet is 255. The bytes that comprise a packet consist of standard asynchronous serial data, which are generated using equipment similar to that used for RS-232C.

5) The packages from MASTER are named request. The packages from SLAVE are named response.

6) Under any circumstance, Slave can just respond one request.

2.2. Modes of Transmission

MODBUS protocol supports ASCII and RTU modes of transmissions. The SPM90 supports only the RTU mode of transmission with 8 data bits, no parity, and one stop bit.

2.3. Description of the Modbus Packet Structure

Every MODBUS packet consists of four fields:

1) The Address Field

2) The Function Field

3) The Data Field

4) The Error Check field

2.3.1 Address Field

The address field is 1-byte long and identifies which slave device the packet is for. Valid addresses range between 1 and 247. The slave device whose address matches the value in this field will perform the command specified in the packet.

2.3.2 Function Field

The function field is 1-byte long and tells the addressed salve which function to perform. Slave response packet should include same function field byte as request. The Modbus functions supported by SPM90 are listed as below:

Function Code	Meaning	Action
0x01	Read Relay Output Status	Obtains ON/ OFF information of one or more relay output in SPM90 (0/1)
0x02	Read Digital Input Status	Obtains ON/OFF information of one or more digital input in SPM90 (0/1)
0x03	Read Holding Registers	Obtains the current value in one or more holding registers of the SPM90.
0x05	Relay control	Write 0xFF00 to close (ON) the relay Write 0x0000 to open (OFF) the relay
0x10	Preset Multiple Registers	Places specific binary values into a series of consecutive holding registers of the SPM90

2.3.3 Data Field

The length of Data Field is varies in length depending on its function. In general, MODBUS supports “BIG INDIAN” mode, it means high-order byte first, low-order byte second.

For example,

One 16 byte register value is 0x12AB; register is transmitted in below sequence:

High-order byte = 0x12

Low-order byte = 0xAB

2.3.4 Error Check Field

In Modbus RTU mode, the 16-bit Cyclic Redundancy Check (CRC-16) is used. The sending device calculates a 16-bit value, based on the information stored in the address, function and data fields using the CRC-16 algorithm and appends it to the end of the packet. The receiving device performs the same calculation upon the reception of a packet. If the result does not match the checksum stored in the packet, transmission errors have occurred and the packet will be ignored by the receiving device.

For detail of CRC16 parity arithmetic, please refer to Section 4 .

2.4. Abnormal Responses

If a Modbus master device sends a non-effective command to a SPM90 or attempts to read a non-effective holding register, an exception response will be generated. The exception response consists of the slave address, function code, error code, and error check field. The high order bit of the function code is set to 1 to indicate that the packet is an exception response.

Below list describes the meanings of exception codes:

Function Code	Meaning
01 illegal function code	SPM90 Modbus support the function code include: 01H, 02H, 03H, 05H, and 10H. This code means the slave device receive an illegal function code, or the SPM90 receive the error command.
02 illegal address	SPM90 receive the address referenced in the data field is an invalid address.
03 illegal address	The requested register number is too long.

2.5. Broadcast Packets

SPM90 support broadcast commands when communicating in MODBUS mode.

Do write command 0x10 for timing.

3. Packet Communication

Two MODBUS functions are supported by the SPM90. The standard MODBUS protocol supports only 16-bit registers, which limit the maximum value of any measurement to 65535.

Section 3.1 will describe the format of Read/ Response Packet of relay output.

Section 3.2 will describe the format of Read/ Response Packet of status input.

Section 3.3 will describe the format of Read/ Response Packet of holding register.

Section 3.4 will describe the relay control command

Section 3.5 will describe Preset Multiple Registers packet and the acknowledge packet.

3.1. Read Holding Registers (Function Code 03H)

This command packet requests that the SPM90 responds all valid registers. The value of reserved registers is 0.

Request Packet (Master→SPM90)		**Response Packet (SPM90→Master)**	
Unit ID/ Slave address	1 byte	Unit ID/ Slave address	1 byte
03 H (Function Code)	1 byte	03 H (Function Code)	1 byte
Start register address	2 bytes	Byte num. (2 * register num.)	1 byte
Registers num.	2 bytes	First register data	2 bytes
CRC check code	2 bytes	Second register data	2 bytes
		... ...	
		CRC check code	2 bytes

3.2. Preset Multiple Registers (Function code 10H)

Preset Registers Format (Master→SPM90)		**Response Format (SPM90→Master)**	
Unit ID/ Slave address	1 byte	Unit ID/ Slave address	1 byte
10 H (Function Code)	1 byte	10 H (Function Code)	1 byte
Start register address	2 bytes	Start register address	2 bytes
Register num.	2 bytes	Register num.	2 bytes
Byte num. (2 * register num.)	1 byte	CRC check code	2 bytes
First register data			
Second register data			
...			
CRC check code	2 bytes		

This command packet allows the Master to program the SPM90 setup parameters.

Note: SPM90 presume all registers are continuous from the first one.

4. Calculating the CRC-16 Error Check Field

This section describes the procedure for obtaining the CRC-16 error check field. A packet can be considered as a continuous, serial stream of binary data (0, 1). The 16-bit checksum is obtained by multiplying the serial data stream by 216 (10000000000000000) and then dividing it by the ***generator polynomial*** $x^{16}+x^{15}+x^2+1$, which can be expressed as a binary data 11000000000000101. The quotient is ignored and the 16-bit remainder is the checksum and is appended to end of the packet.

In calculating the CRC, all arithmetic operations (additions and subtractions) are performed using MODULO TWO, or EXCLUSIVE OR operation.

Steps for the Generating the CRC-16 Checksum:

1) Form a new polynomial by dropping the MSB (Most Significant Bit) of the generator polynomial and reversing the bit sequence. This yields the binary number 1010 0000 0000 0001 or A0 01 Hex.

2) Load a 16-bit register with initial value FF FF Hex.

3) Exclusive OR the first data byte with the loworder byte of the 16-bit register, storing the result in the 16-bit register.

4) Shift the 16-bit register one bit to the right. If overflow bit is 1, then turn to step 5). Otherwise, turn to step 6)

5a) If the bit shifted out to the right is one, Exclusive OR the 16-bit register with the new generator polynomial, with result stored in the16-bit register. Return to step 4.

5b) If the bit shifted out to the right is zero, return to step 4.

6) Repeat steps 4 and 5 until 8 shifts have been performed.

7) Exclusive OR the next data byte with the 16-bit register.

8) Repeat steps 4 through 7 until all bytes of the packet have been calculate by XOR

9) The content of the 16-bit register is CRC-16

Procedure for Calculating the 6403 Bytes of 16 Hex.

Step	Byte	Action	Register	Bit #	Shift
2		Initial Value	1111 1111 1111 1111		
	1	Load the first byte	0000 0000 0110 0100		
3		XOR	1111 1111 1001 1011		
4		SHIFT 1 bit to the right	0111 1111 1100 1101	1	1
5a		XOR polynomial	1101 1111 1100 1100		
4		SHIFT 1 bit to the right	0110 1111 1110 0110	2	0
4		SHIFT 1 bit to the right	0011 0111 1111 0011	3	0
4		SHIFT 1 bit to the right	0001 1011 1111 1001	4	1
5a		XOR polynomial	1011 1011 1111 1000		
4		SHIFT 1 bit to the right	0101 1101 1111 1100	5	0
4		SHIFT 1 bit to the right	0010 1110 1111 1110	6	0
4		SHIFT 1 bit to the right	0001 0111 0111 1111	7	0
4		SHIFT 1 bit to the right	0000 1011 1011 1111	8	1
5a		SHIFT 1 bit to the right	1010 1011 1011 1110		
	2	Load the second byte	0000 0000 0000 0011		
7		XOR	1010 1011 1011 1101		
4		SHIFT 1 bit to the right	0101 0101 1101 1110	1	1
5a		XOR polynomial	1111 0101 1101 1111		
4		SHIFT 1 bit to the right	0111 1010 1110 1111	2	1
5a		XOR polynomial	1101 1010 1110 1110		
4		SHIFT 1 bit to the right	0110 1101 0111 0111	3	0
4		SHIFT 1 bit to the right	0011 0110 1011 1011	4	1
5a		XOR polynomial	1001 0110 1011 1010		
4		SHIFT 1 bit to the right	0100 1011 0101 1101	5	0
4		SHIFT 1 bit to the right	0010 0101 1010 1110	6	1
5a		XOR polynomial	1000 0101 1010 1111		
4		SHIFT 1 bit to the right	0100 0010 1101 0111	7	1
5a		XOR polynomial	1110 0010 1101 0110		
4		SHIFT 1 bit to the right	0111 0001 0110 1011	8	0

		CRC-16	0111 0001 0110 1011		

5. Description of SPM90 Registers

All SPM90 measured and setup parameters are treated as HOLDING REGISTERS having addresses **4xxxx** when communicating in MODBUS protocol. According to the MODBUS Protocol, in response to a request for register **4xxxx** of a particular slave device (SPM90), the MODBUS master reads register **xxxx-1** from the slave (SPM90). For example register 40011 corresponds to register 10.

6. Register Lists

Access and Type of Register

Items	Access and Type	Description
1	RO	Read only
2	WO	Write only
3	RW	Read or Write
4	U16	16 bit, un-sign integer
5	S16	16 bit, sign integer
6	U32	32 bit, un-sign integer
7	S32	32 bit, sign integer
8	WORD16	Bit denotation word, applicable to digital input and relay status.

6.1 Real-time data register list

Register address	Access	Type	Description	Remark
40001	RO	U16	Voltage	Calculation factor 0.1, Unit V
40002	RO	U16	Current	Calculation factor 0.01，Unit A
40003	RO	U16	Active power high bit	Active power，Calculation factor 1，Unit: W
40004	RO	U16	Active power low bit	
40005	RO	U16	Active Energy high bit	Active energy，Calculation factor 0.01，Unit: kWh
40006	RO	U16	Active Energy low bit	
40007	RO	U16	Voltage Measure Direction	0 means measure voltage forward direction 1 means measure voltage reverse direction

6.4 List of configuration registers

Register address	Access	Type	Description	Remark
41001	RW	U16	Communication Address	1- to 247
41002	RW	U16	Baud rate	0 to 3 0-2400 1-4800 2-9600 3-19200
41003	RW	U16	Protocol	0：MODBUS 1：DLT645
41004	RW	U16	Reversed	
41005	RW	U16	Reversed	
41006	RO	U16	Reversed	
41007	RW	U16	DLT645 Address byte 1、0	0-9999
41008	RW	U16	DLT645 Address byte 3、2	0-9999
41009	RW	U16	DLT645 Address byte 5、4	0-9999
41010	RW	U16	Password Byte 1、0	0-9999
41011	RW	U16	Password Byte 3、2	0-9999

PILOT reserves the right to modify this manual without prior notice in view of continued improvement

Zhuhai Pilot Technology Co., Ltd.

Add:No.15,keji6Road,Chuangxin Haian,Tangjia High-tech Zone,Zhuhai,Guangdong,519085 China

Tel: +86-756-3629687/3629688

Fax: +86-756-3629600/3629670

http://www.pmac.com.cn