9900标准电量监测仪

MODBUS串行通信协议

ZHUHAI PILOT ELECTRONICS Co.,Ltd

Doc.No.03-0304-002

目　　录

第一章　简 介

通信协议详细地描述了 9900 在 MODBUS 通讯模式下的输入和输出命令、信息和数据，以便第三方使用和开发。

1．1 串行通讯协议的目的

通信协议的作用使信息和数据在上位机（主站）和 9900 之间有效地传递，它包括：

1） 允许主站访问和设定所接 9900 的全部设置参数；

2） 允许访问 9900 的所有测量数据和事件纪录。

1．2 MODBUS 通讯协议的版本

该通讯协议适用于本公司已经出厂的所有各种版本的 9900 仪表，对于日后的系列若有改动会加以特别说明。

第二章　9900-MODBUS 串行通信协议详细说明

2．1 9900-MODBUS 协议基本规则

以下规则确定在 RS485（或者 RS232C）回路控制器和其他 RS485 串行通信回路中设备的通信规则：

1）所有 RS485 回路通信应遵照主/从方式。在这种方式下，信息和数据在单个主站和最多 32 个从站（监控设备）之间传递；

2）主站将初始化和控制所有在 RS485 通信回路上传递的信息；

3）无论如何都不能从一个从站开始通信；

4）所有 RS485 环路上的通信都以“打包”方式发生。一个包裹就是一个简单的字符串（每个字符串 8 位），一个包裹中最多可含 255 个字节。组成这个包裹的字节构成标准异步串行数据，并按 8 位数据位，1 位停止位，无校验位的方式传递。串行数据流由类似于 RS232C 中使用的设备产生；

5）主站发送包裹称为请求，从站发送包裹称为响应；

6）任何情况从站只能响应主站一个请求。

2．2 传送模式

MODBUS 协议可以采用 ASCII 或者 RTU 模式传送数据。9900 仅仅支持 RTU 模式，8 位数据位，无校验位，1 位停止位。

2．3 MODBUS 包裹结构描述

每个 MODBUS 包裹都由以下几个部分组成：

1） 地址域

2） 功能码域

3） 数据域

4） 校验域

2．3．1 地址域

MODBUS 的从站地址域长度为一个字节，包含包裹传送的从站地址。有效的从站地址范围从 1~247。从站如果接收到一帧从站地址域信息与自身地址相符合的包裹时，应当执行包裹中所包含的命令。从站所响应的包裹中该域为自身地址。

2．3．2 功能码域

MODBUS 包裹中功能域长度为一个字节，用以通知从站应当执行何操作。从站响应包裹中应当包含主站所请求操作的相同功能域字节。有关 9900 的功能码参照下表。

功能码	含义	功能
0x03	读取寄存器	获得当前 9900 内部一个或多个当前寄存器值
0x10	设置寄存器	将指定数值写入 9900 内部一个或多个寄存器内

2．3．3 数据域

MODBUS 数据域长度不定，依据其具体功能而定。MODBUS 数据域采用”BIG INDIAN”模式，即是高位字节在前，低位字节在后。举例如下：

Example 2.1

1 个 16 位寄存器包含数值为 0x12AB，寄存器数值发送顺序为：

高位字节 = 0x12

低位字节 = 0x0AB

2．3．4 校验域

MODBUS-RTU 模式采用 16 位 CRC 校验。发送设备应当对包裹中的每一个数据都进行 CRC16 计算，最后结果存放入检验域中。接收设备也应当对包裹中的每一个数据（除校验域以外）进行 CRC16 计算，将结果域校验域进行比较。只有相同的包裹才可以被接受。具体的 CRC 校验算法参照附录。

2．4 网络时间考虑

在 RS485 网络上传送包裹需要遵循以下有关时间的规定：

1） 主站请求包裹结束到从站响应包裹开始之间的时间最小为 20 毫秒，最大为 250 毫秒，典型值为 60 毫秒；

2） 从站响应包裹结束到主站下一请求包裹开始之间的时间在 16 位模式下典型值为 100 毫秒，在 32 位模式下典型值为 500 毫秒；

3） 包裹中相邻两个字节之间的最大时间依据通讯波特率不同而不同，一般来说最大字节时间为 3 倍的字节发送时间（例如 9600 波特率下，字节间隔为 3 毫秒；4800 波特率时，字节间隔为 6 毫秒）。

2．5 异常响应

如果主站发送了一个非法的包裹给 9900 或者是主站请求一个无效的数据寄存器时，异常的数据响应就会产生。这个异常数据响应由从站地址、功能码、故障码和校验域组成。当功能码域的高比特位置为 1 时，说明此时的数据帧为异常响应。下表说明异常功能码的含义：

功能码名称	说明
01 非法功能码	The 9900 9900-MODBUS 只支持 03H 和 10H 功能码，该码表示从站接收到非法的功能码；或者是 9900 接收到一个错误的操作密码。
02 非法数据地址	说明 9900 接收到无效的数据地址，或者是请求寄存器不在有效的寄存器范

围内。

2．6 广播命令

9900-MODBUS 协议不支持广播命令。

第三章　通 讯 包 裹

9900-MODBUS 支持两个功能码，标准的 MODBUS 协议仅支持 16 位数据模式，也就说传输任何测量值最大为 65535。为了支持传输更大的测量值，9900 提供了扩展的 32 位数据模式。

3.1 节将描述 16 位数据模式与 32 位数据模式的不同。3.2 节将说明 9900 的读数据包裹和响应包裹的格式。3.3 节将说明 9900 写数据包裹和响应包裹的格式。

3．1 16 位/32 位数据通讯模式

16位数据模式中，所有的数据都是通过一个16位寄存器表示，即使实际数值超过65535，但是传输的最大值只能为65535。32位模式中，所有的数据都是依照如下规则组织的：

1） 除电能参数以外的实时数据和设置参数都是用两个寄存器说明：

高位寄存器 = 实际值 / 10000 （商值）

低位寄存器 = 实际值 / 10000 （余数）

这种设定方式是为了兼容MODICON的PLC装置；

2）符号寄存器，高位寄存器固定位0，低位寄存器仍然保持原有数据；

3）电能数据不论采用16位或者32位数据模式，都可以采用两个寄存器表示：

16位数据模式：

高16位 = 实际值 / 1000 （商值）

低16位 = 实际值 / 1000 （余数）

32位数据模式:

高32位寄存器：

高16位 = 0

第16位 = 实际值 / 1000000 （商值）

低32位寄存器：

高16位 = （实际值 / 10000） / 100 （余数）

低16位 = 实际值 / 10000 （余数）

在16位数据模式下，电能数据最大为65000MWH；在32位数据模式下，电能数据最大为2000GWH。

3．2 读寄存器（功能码 03）

由主站机发送的包裹请求 9900 响应所有有效的寄存器（在起始寄存器和终止寄存器之间）。一般读寄存器不需要密码，但在以下两种情况下需要正确的密码。

1） 去读一个被保护的寄存器：目前唯一被保护的寄存器是保护仪表密码的寄存器。

2） 如果“只读保护”寄存器（地址 43017）已设置，那么密码正确才能读任何寄存器。

在响应包裹中仅仅有效的寄存器才能被发送。9900 没有配置的寄存器或对该输入电压模式下不存在的寄存器将不被发送。

由于MODBUS协议中并没有专门的密码域，所以执行与密码相关的操作时需要执行一个特殊的操作。

首先采用写寄存器功能码将密码写入到密码寄存器中（地址 43051）。无论写入密码是

否正确，9900 都会做出响应。此时用户在执行需要操作的功能。如果先前的写入密码不正确，则响应的包裹为异常，如果写入密码正确，则 9900 会响应正常的数据。

16 位模式

读寄存器包裹格式（主机→9900）			响应格式（9900→主机）	
从站地址	1 字节		从站地址	1 字节
功能码 03H	1 字节		功能码 03H	1 字节
开始地址	2 字节		字节数（2*寄存器数目）	1 字节
寄存器个数	2 字节		第一个寄存器数据	2 字节
CRC 校验码	2 字节		第二个寄存器数据	2 字节
			……	
			CRC 校验码	2 字节

32 位模式

读寄存器包裹格式（主机→9900）			响应格式（9900→主机）	
从站地址	1 字节		从站地址	1 字节
功能码 03H	1 字节		功能码 03H	1 字节
开始地址	2 字节		字节数（2*寄存器数目）	1 字节
寄存器个数	2 字节		第一个寄存器数据高位字	2 字节
CRC 校验码	2 字节		第一个寄存器数据低位字	2 字节
			第二个寄存器数据高位字	2 字节
			第二个寄存器数据低位字	2 字节
			……	
			CRC 校验码	2 字节

注意

1） 响应包裹中只会包含有效的寄存器，那些未配置的寄存器和无效的寄存器都不会被仪表发送上来。所以用户首先要确定仪表中所配置的寄存器。例如，如果用户需要请求 40046 寄存器数据，如果 9900 并未配置该寄存器，则仪表将会将 40055 寄存器数据送上。（假定仪表在 40046 寄存器后配置的第一个有效寄存器是 40055）；

2） 32 位数据模式下，请求寄存器数目是 16 位数据模式下的 2 倍。例如，在 32 位模式下请求 10 个参数需要 20 个寄存器，但在 16 位模式下只需要 10 个寄存器；

3．3 写寄存器（功能码 16）

该命令允许主站配置 9900 工作参数，以下为数据格式：

16 位模式

写寄存器包裹格式（主机→9900）			响应格式（9900→主机）	
从站地址	1 字节		从站地址	1 字节
功能码 10H	1 字节		功能码 10H	1 字节
开始地址	2 字节		开始地址	2 字节
寄存器个数	2 字节		寄存器个数	2 字节
字节个数（2*寄存器个数）	1 字节		CRC 校验码	2 字节
第一个寄存器数据				
第二个寄存器数据				
…….				
CRC 校验码	2 字节			

32 位模式

写寄存器包裹格式（主机→9900）			响应格式（9900→主机）	
从站地址	1 字节		从站地址	1 字节
功能码 10H	1 字节		功能码 10H	1 字节
开始地址	2 字节		开始地址	2 字节
寄存器个数	2 字节		寄存器个数	2 字节
字节个数（2*寄存器个数）	1 字节		CRC 校验码	2 字节
第一个寄存器数据高位字				
第一个寄存器数据低位字				
第二个寄存器数据高位字				
第二个寄存器数据低位字				
…….				
CRC 校验码	2 字节			

注意

1） 9900假定写入的寄存器从第一个寄存器开始是连续的；

2） 32位模式下，写入的寄存器数目是16位模式的两倍，例如，在32位模式下写10个参数需要20个寄存器，而在16位模式下只需要10个寄存器；

第四章　计算 CRC-16

该部分将描述计算ＣＲＣ－１６的过程。在帧中的有关的字节被义为是一串 2 进制数据（０，１）。第１６位校验和是这样得到的：该串数据流被２１６乘，然后除以发生器多项式（$X^{16}+X^{15}+X^{2}+1$），该式以 2 进制表示为 1100000000000101。商被忽略，１６位的余数就是ＣＲＣ的值，在计算ＣＲＣ－１６值时，全部算术运算用 modulo two 或者异或（X0R）算法。

按照下列步骤产生 CRC-16 的校验和：

1）省略发生器最有意义的位，并且把位的顺序颠倒过来。形成一个新的多项式，结果是 1010000000000001 或者 16 进制的 A001。

2）将全部 1 或者 16 进制 FFFF 装入 16 位寄存器。

3）用 16 位寄存器中低阶字节对第一个数据字节进行 XOR 运算，把结果存入 16 位寄存器。

4）把 16 位寄存器向右移一位。如果溢出位为 1，则转向第 5 步骤，否则转向第 6 步骤。

5）用新的发生器多项式对 16 位寄存器执行 MOR 运算，并且把结果存入 16 步骤。

6）重复步骤 4，直到移位 8 次为止。

7）用 16 位寄存器的第阶字节对下一个数据字节进行 XOR 运算，将结果存入 16 位寄存器。

8）重复步骤 4-7，直到小包的所有字节都已经用 16 位寄存器执行了 XOR 运算为止。

9）16 位寄存器的内容就是 CRC-16

下面的例子是对 16 进制的 **6403** 这个字节进行 CRC 计算。

步骤	字节	动作	寄存器	位#	移位
2		初值	1111 1111 1111 1111		
	1	装入第一字节	0000 0000 0110 0100		
3		异或	1111 1111 1001 1011		
4		右移一位	0111 1111 1100 1101	1	1
5a		异或多项式	1101 1111 1100 1100		
4		右移一位	0110 1111 1110 0110	2	0
4		右移一位	0011 0111 1111 0011	3	0
4		右移一位	0001 1011 1111 1001	4	1
5a		异或多项式	1011 1011 1111 1000		
4		右移一位	0101 1101 1111 1100	5	0
4		右移一位	0010 1110 1111 1110	6	0
4		右移一位	0001 0111 0111 1111	7	0
4		右移一位	0000 1011 1011 1111	8	1
5a		异或多项式	1010 1011 1011 1110		
	2	装入第二字节	0000 0000 0000 0011		
7		异或	1010 1011 1011 1101		
4		右移一位	0101 0101 1101 1110	1	1
5a		异或多项式	1111 0101 1101 1111		
4		右移一位	0111 1010 1110 1111	2	1

5a		异或多项式	1101 1010 1110 1110		
4		右移一位	0110 1101 0111 0111	3	0
4		右移一位	0011 0110 1011 1011	4	1
5a		异或多项式	1001 0110 1011 1010		
4		右移一位	0100 1011 0101 1101	5	0
4		右移一位	0010 0101 1010 1110	6	1
5a		异或多项式	1000 0101 1010 1111		
4		右移一位	0100 0010 1101 0111	7	1
5a		异或多项式	1110 0010 1101 0110		
4		右移一位	0111 0001 0110 1011	8	0
		CRC-16	0111 0001 0110 1011		

第五章　9900 寄存器说明

所有的 9900 寄存器（包括实时寄存器和设置寄存器），在 MODBUS 通讯协议时都具有 4XXXX 的基址。根据 MODBUS 协议，请求 9900 中一个地址为 4XXXX 的寄存器时，主站实际读取为 XXXX-1。例如，请求 9900 中 40011 寄存器，主站实际寄存器号为 10。

下表说明在不同电压模式下，部分实时寄存器的状态发生了变化，原有的有效寄存器变为无效。

寄存器		电压模式	
寄存器	描述	WYE，DEMO	3-WIRE DELTA
40011	A 相电压	有效	无效
40012	B 相电压	有效	无效
40013	C 相电压	有效	无效
40014	相电压平均值	有效	无效
40031	A 相有功功率	有效	无效
40032	B 相有功功率	有效	无效
40033	C 相有功功率	有效	无效
40035	A 相无功功率	有效	无效
40036	B 相无功功率	有效	无效
40037	C 相无功功率	有效	无效
40039	A 相功率因数	有效	无效
40040	B 相功率因数	有效	无效
40041	C 相功率因数	有效	无效
40043	A 相视在功率	有效	无效
40044	B 相功率因数	有效	无效
40045	C 相功率因数	有效	无效

附录 A 9900-MODBUS寄存器表格

表 F –1 9900 数据寄存器

寄存器号	寄存器类型	描述	标准配置（Basic） 可选 （Optical）
40011	RO	A 相相电压	Basic
40012	RO	B 相相电压	Basic
40013	RO	C 相相电压	Basic
40014	RO	相电压平均值	Basic
40015	RO	AB 线电压	Basic
40016	RO	BC 线电压	Basic
40017	RO	CA 线电压	Basic
40018	RO	线电压平均值	Basic
40021	RO	A 相电流	Basic
40022	RO	B 相电流	Basic
40023	RO	C 相电流	Basic
40024	RO	相电流平均值	Basic
40031	RO	A 相有功功率	Basic
40032	RO	B 相有功功率	Basic
40033	RO	C 相有功功率	Basic
40034	RO	三相有功功率	Basic
40035	RO	A 相无功功率	Basic
40036	RO	B 相无功功率	Basic
40037	RO	C 相无功功率	Basic
40038	RO	三相无功功率	Basic
40039	RO	A 相功率因数	Basic
40040	RO	B 相功率因数	Basic
40041	RO	C 相功率因数	Basic
40042	RO	功率因数总计	Basic
40043	RO	A 相视在功率	Basic
40044	RO	B 相视在功率	Basic
40045	RO	C 相视在功率	Basic
40046	RO	三相视在功率	Basic
40048	RO	系统频率	Basic
40050	RO	符号寄存器	Basic
40051	RO	有功电度输入 KWH	Basic
40052	RO	有功电度输入 MWH	Basic

40053	RO	有功电度输出 KWH	Basic
40054	RO	有功电度输出 MWH	Basic
40055	RO	有功电度净值 KWH	Basic
40056	RO	有功电度净值 MWH	Basic
40061	RO	无功电度输入 KVARH	Basic
40062	RO	无功电度输入 MVARH	Basic
40063	RO	无功电度输出 KVARH	Basic
40064	RO	无功电度输出 MVARH	Basic
40065	RO	无功电度净值 KVARH	Basic
40066	RO	无功电度净值 MVARH	Basic
40071	RO	视在电度净值 KVAH	Basic
40072	RO	视在电度净值 MVAH	Basic

表 F-2 特殊功能寄存器

寄存器号	**寄存器类型**	**描述**	**标准配置（Basic） 可选 （Optical）**
43002	RW	PT 一次侧电压	Basic
43003	RW	PT 二次侧电压	Basic
43004	RW	CT 一次侧电流	Basic
43005	RW	C 电压输入模式 （0，1，2，3 或 4）	Basic
43006	RW	设备号	Basic
43007	RW	波特率（300，1200，2400，4800，9600，19200）	Basic
43008	保留		
43009	RW	对比度视觉调节	Basic
43010	RW	密码	Basic
43011	WO	复位所有最小/最大值	Basic
43012	WO	复位所有时间计数器（如：千瓦时）	Basic
43013	RO	版本号	Basic
43014	RO	最新版本日期	Basic
43015	RO	特征码	Basic
43016	RO	设备类型	Basic
43017	RW	允许只读保护 （YES OR NO）	Basic
43018	保留		
43051	WO	包裹密码	Basic

符号寄存器含义

由于MODBUS数据为16位无符号字，所以当用户需要判断功率以及电度的正负情况时，就必须借助于符号寄存器进行，以下为符号寄存器的定义：

位号	寄存器	位号	寄存器
D0	40031	D1	40032
D2	40033	D3	40034
D4	40035	D5	40036
D6	40037	D7	40038
D8	40039	D9	40040
D10	40041	D11	40042
D12	无效	D13	无效
D14	40055,40056	D15	40065,40066

相应位为1说明对应的寄存器数据符号为负，为0说明为正。