MODBUS 协议

1. 读取线圈状态（功能码＝01）

读从机设备离散量输出口的 ON/OFF 状态，不支持广播。

查询信息规定了要读的起始线圈和线圈量，线圈的起始地址为零，1－16 个线圈的寻址地址分别为 0－15。表 1 列出控制器支持最大的参数清单。

响应信息中的各线圈的状态与数据区的每一位的值相对应，1＝ON；0＝OFF。第一个数据字节的 LSB（最低有效字符）为查询中的寻址地址，其他的线圈按顺序在该字节中由低位高位排列，直至 8 个为止，下一个字节也是从低位向高位排列。

若返回的线圈数不是 8 的倍数，则在最后的数据字节中的剩余位至字节的最高位全部填零，字节数区说明全部数据的字节数。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x01
开始地址	2 字节	0x00－0xFFFF
线圈数量	2 字节	1－2000（0x7D0）
校验码	2 字节	

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x01
线圈数量对应的字节数	1 字节	N
线圈数据 1 (Coils 27－Coils 20)	1 字节	
线圈数据 2 (Coils 2F－Coils 28)	1 字节	
线圈数据 n (Coils 32－Coils 30)	1 字节	n=N 或 N＋1
校验码	2 字节	

如果线圈数量是 8的位数，则 N= n/8，否则 N= N+ 1

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x81
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

2. 读取输入状态（功能码＝02）

读从机设备离散量输入信号的 ON/OFF 状态。不支持广播。

查询信息规定了要读的输入起始地址，以及输入信号的数量。输入起始地址为 0，1－16 个输入口的地址分别为 0－15。表 1 列出控制器支持最大的参数清单。

响应信息中的各输入口的状态，分别对应于数据区中的每一位值，1＝ON；0＝OFF，第一个数据字节的 LSB（最低有效字符）为查询中的寻址地址，其他输入口按顺序在该字节中由低位向高位排列，直至 8 个位为止。下一个字节中的 8 个输入位也是从低位到高位排列。

若返回的输入位数不是 8 的倍数，则在最后的数据字节中的剩余位直至字节的最高位全部填零。字节的最高位字节数区。说明了全部数据的字节数。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x02
开始地址	2 字节	0x00－0xFFFF
离散数据数量	2 字节	1－2000（0x7D0）
校验码	2 字节	

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x02
离散状态数量对应的字节数	1 字节	N
离散数据 1 (Inputs 10204－Inputs 10197)	1 字节	
离散数据 2 (Inputs 10212－Inputs 10205)	1 字节	
离散数据 n (Inputs 10218－Inputs 10213)	1 字节	n=N 或 N＋1
校验码	2 字节	

如果离散输入数据数量是 8的位数，则 N＝n/8，否则 N＝N＋1

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x82
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

3. 读保持寄存器（功能码＝03）

读从设备保持寄存器（4X 类型）中的二进制数据，不支持广播。

查询信息规定了要读的寄存器起始地址及寄存器的数量，寄存器寻址起始地址为 0000，寄存器 1－16 所对应的地址分别为 0－15。

响应信息中的寄存器数据为二进制数据，每个寄存器分别对应 2 个字节，第一个字节为高位数据，第二个字节为低位数据。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x03
开始地址	2 字节	0x00－0xFFFF
寄存器数量	2 字节	1－125（0x7D）
校验码	2 字节	

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x03
保持寄存器数量对应的字节数	1 字节	2*N
寄存器数值 1	2 字节	
寄存器数值 2	2 字节	
寄存器数值 n	2 字节	n=N
校验码	2 字节	

N＝寄存器数量

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x83
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

4. 读取输入寄存器（功能码＝04）

读从机设备输入寄存器（3X 类型）中的二进制数据，不支持广播。

查询信息规定了要读的寄存器的起始地址及寄存器的数量，寻址起始地址为 0000，寄存器 1－16 所对应的地址分别为 0－15。表 1 列出控制器支持最大的参数清单。

响应信息中的寄存器数据为每个寄存器分别对应 2 个字节，第一个字节为高位数据，第二个字节为低位数据。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x04
开始地址	2 字节	0x00－0xFFFF
输入寄存器数量	2 字节	1－125（0x7D）
校验码	2 字节	

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x04
输入寄存器数量对应的字节数	1 字节	2*N
输入寄存器数值 1	2 字节	
输入寄存器数值 2	2 字节	
输入寄存器数值 n	2 字节	n=N
校验码	2 字节	

N＝输入寄存器数量

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x84
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

5. 强置单个线圈（功能码＝05）

强制单个线圈（0X 类型）为 ON 或 OFF 状态。广播时该功能可强制所有从机中同一类型的线圈均为 ON 或 OFF 状态。表 1 列出控制器支持最大的参数清单。

注意：该功能可越过控制器内存的保护状态和线圈的禁止状态。线圈强制状态一直保持有效直至下一个控制逻辑作用于线圈为止。控制逻辑中无线圈程序时，则线圈处于强制状态。

查询信息规定了需要强制线圈的类型，线圈起始地址为 0，线圈 1 的寻址地址为 0。由查询数据区中的一个常量。规定被请求线圈的 ON/OFF 状态，FF00H 值请求线圈处于 ON 状态，0000H 值请求线圈处于 OFF 状态，其它值对线圈无效，不起作用。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x05
输出地址	2 字节	0x00－0xFFFF
线圈数值	2 字节	0x00 或 0xFF00
校验码	2 字节	

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x05
输出地址	2 字节	0x00－0xFFFF
线圈数值	2 字节	0x00 或 0xFF00
校验码	2 字节	

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x85
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

6. 预置单个寄存器（功能码＝06）

把一个值预置到一个 4X 类型保持寄存器中。广播时该功能把值预置到所有从机的相同类型的寄存器中。

注意：该功能可越过控制器的内存保护。使寄存器中的预置值保持有效。只能由控制器的下一个逻辑信号来处理该预置值。若控制逻辑中无寄存器程序时，则寄存器中的值保持不变。

查询信息规定了要预置寄存器的类型，寄存器寻址起始地址为 0，寄存器 1 所对应的地址为 0。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x06
寄存器地址	2 字节	0x00－0xFFFF
寄存器数值	2 字节	0x00－0xFFFF
校验码	2 字节	

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x06
寄存器地址	2 字节	0x00－0xFFFF
寄存器数值	2 字节	0x00－0xFFFF
校验码	2 字节	

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x86
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

7. 强置多个线圈（功能码＝15）

按线圈的顺序把各线圈（0X 类型）强制成 ON 或 OFF。广播时，该功能代码可对各从机中相同类型的线圈起强制作用。表 1 列出控制器支持最大的参数清单。

注意：该功能代码可越过内存保护和线圈的禁止状态线圈。保持强制状态有效，并只能由控制器的下一个逻辑来处理。若无线圈控制逻辑程序时，线圈将保持强制状态。

查询信息规定了被强制线圈的类型，线圈起始地址为 0，线圈 1 寻址地址为 0。

查询数据区规定了被请求线圈的 ON/OFF 状态，如数据区的某位值为“ 1 ”表示请求的相应线圈状态为 ON，位值为“ 0 ”，则为 OFF 状态。

下述例子为请求从机设备 17 中一组 10 个线圈为强制状态，起始线圈为 20（则寻址地址为 19 或 13H），查询的数据为 2 个字节，CD01H（二进制 11001101 0000 0001）相应线圈的二进制位排列如下：

Bit: 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1

Coll: 27 26 25 24 23 22 21 20 - - - - - - - - 29 28

传送的第一个字节 CDH 对应线圈为 27-20, LSB 对应线圈 20，传送的第二个字节为 01H，对应的线圈为 29-28，LSB 为继圈 28，其余未使用的位均填“ 0 ”。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x0F
开始地址	2 字节	0x00－0xFFFF
线圈输出数量	2 字节	0x0001－0x07B0
线圈数量对应的字节数	1 字节	N
线圈输出数据 1 (Coils 27－Coils 20)	1 字节	
线圈输出数据 2 (Coils 2F－Coils 28)	1 字节	
线圈输出数据 n (Coils 32－Coils 30)	1 字节	n=N 或 N＋1
校验码	2 字节	

如果线圈数量是 8 的位数，则 N＝n/8，否则 N＝N＋1

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x0F
开始地址	2 字节	0x00－0xFFFF
线圈输出数量	2 字节	0x0001－0x07B0
校验码	2 字节	

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	

功能码	1 字节	0x8F
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

名称	例如
设备地址	11
功能码	0F
开始地址 Hi	00
开始地址 Lo	14
线圈输出数量 Hi	00
线圈输出数量 Lo	0A
线圈数量对应的字节数	02
线圈输出数据 1 (Coils 27－Coils 20)	CD
线圈输出数据 2 (Coils 29－Coils 28)	01
校验码	----

8. 预置多个寄存器（功能码＝16）

把数据按顺序预置到各（4×类型）寄存器中，广播时该功能代码可把数据预置到全部从机中的相同类型的寄存器中。

注意：该功能代码可越过控制器的内存保护，在寄存器中的预置值一直保持有效，只能由控制器的下一个逻辑来处理寄存器的内容，控制逻辑中无该寄存器程序时，则寄存器中的值保持不变。

信息中规定了要预置的寄存器类型，寄存器寻址的起始地址为 0，寄存器 1 寻址地址为 0。查询数据区中指定了寄存器的预置值。寄存器数据为每个寄存器分别对应 2 个字节，第一个字节为高位数据，第二个字节为低位数据。

正常响应返回从机地址，功能代码和起始地址和预置寄存器数。

n 主机请求报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x10
开始地址	2 字节	0x00－0xFFFF
寄存器数量	2 字节	0x01－0x0078
寄存器数量对应的字节数	1 字节	2*N
寄存器数值 1	2 字节	
寄存器数值 2	2 字节	
寄存器数值 n	2 字节	
校验码	2 字节	

N＝寄存器数量

n 从设备应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x10
开始地址	2 字节	0x00－0xFFFF
寄存器数量	2 字节	0x0001－0x007B
校验码	2 字节	

n 从设备错误应答报文：

名称	长度	说明
设备地址	1 字节	
功能码	1 字节	0x90
错误码	1 字节	错误码为 01 或 02 或 03 或 04
校验码	2 字节	

9. MODBUS 协议

9.1. MODBUS 协议编码规则

MODBUS-RTU 的规定，寄存器为 16 位双字节寄存器，采用高字节在前，低字节在后的次序排列。

9.2. MODBUS 数据类型

名称	长度	属性	说明
离散输入	1 位（BIT）	只读	
线圈	1 位（BIT）	读/写	
输入寄存器	16 位（WORD）	只读	
保持寄存器	16 位（WORD）	读/写	

9.3. MODBUS 最大查询/响应参数

功能码	说明	查询	响应
1	读线圈状态	2000 线圈	2000 线圈
2	读输入状态	2000 输入	2000 输入
3	读保持寄存器	125 寄存器	125 寄存器
4	读输入状态	125 寄存器	125 寄存器
5	强置单线圈	1 线圈	1 线圈
6	预置单寄存器	1 寄存器	1 寄存器
15	强置多线圈	800 线圈	800 线圈
16	预置多寄存器	100 寄存器	100 寄存器

表 1　MODBUS 最大查询/响应参数

9.4. MODBUS 故障码

故障码	名称	说明
1	不合法功能代码	从机接收的是一种不能执行功能代码。发出查询命令后，该代码指示无程序功能。
2	不合法数据地址	接收的数据地址，是从机不允许的地址。
3	不合法数据	查询数据区的值是从机不允许的值。
4	执行命令出错	从机执行主机请求的动作时出现不可恢复的错误。
5	执行时间超时错误	从机已接收请求处理数据，但需要较长的处理时间，为避免主机出现超时错误而发送该确认响应。主机以此再发送一个“查询程序完成”未决定从机是否已完成处理。
6	从设备忙	从机正忙于处理一个长时程序命令，请求主机在从机空闲时发送信息。
7	无法执行的命令	
8	偶校验错误	从机内存中的数据，发现有奇偶校验错误。

9.5. MODBUS-RTU 帧的基本格式

起始位	设备地址	功能码	数据区	错误校验	结束符
T1-T2-T3-T4	1 个字节	1 个字节	多个字节	2 个字节	T1-T2-T3-T4

RTU 模式中，信息开始至少需要有 3.5 个字符的静止时间（如上图中的 T1-T2-T3-T4），接着，第一个区的数据为设备地址。各个区允许发送的字符均为 16 进制的 0－9，A－F。网络上的设备连续监测网络上的信息，包括静止时间。当接收第一个地址数据时，每台设备立即对它解码，以决定是否是自己的地址。

发送完最后一个字符号后，也有一个 3.5 个字符的静止时间，然后才能发送一个新的信息。

整个信息必须连续发送。如果在发送帧信息期间，出现大于 1.5 个字符的静止时间时，则接收设备刷新不完整的信息，并假设下一个地址数据。

发送一个信息后，立即发送的一个新信息，（若无 3.5 个字符的静止时间）这将会产生一个错误。是因为合并信息的 CRC 校验码无效而产生的错误。

n 设备地址

从设备地址占用 1 字节，有效的从设备地址范围为 0－247（十进制），各从设备的寻址范围为 1－247。主机把从机设备地址放入信息帧的地址区，并向从机寻址。从机响应时，把自己的地址放入响应信息的地址区，让主机识别自己做出响应的从机地址。

地址 0 是广播地址，所有从机设备均能识别。

n 功能码

信息帧功能代码有效码范围为 1－225（十进制），当主机向从句发送信息时，功能代码向从机说明应执行的动作。当从机响应主机时，功能代码可说明从机正常响应或出现错误（即不正常响应），正常响应时，从机简单返回原始功能代码；不正常响应时，从机返回与原始代码相等效的一个码，并把最高有效位设定为“ 1 ”。

n 数据区

数据区的结构和长度按不同的功能来具体确定。MODBUS-RTU 模式数据采用 16 进制形式，数据的排列采用“ DING　INDIAN ”模式，即高位字节在前，低位字节在后。

n 错误校验

MODBUS-RTU 模式采用 16 位 CRC 校验。发送设备对发送帧中的每一个数据都进行 CRC16 计算，最后将结果存放到错误校验域中。接收设备也对接收帧中的每一个数据除错误校验域以外的数据进行 CRC16 计算，将结果和校验进行比较，只有校验相同，接收帧才被确。