ModBus RTU 协议

主机请求						
地址	功能码	第一个寄存器的高位地址	第一个寄存器的低位地址	寄存器的数量的高位	寄存器的数量的底位	错误校验
01	03	00	38	00	01	XX
从机应答						
地址	功能码	字节数	数据高字节	数据低字节	错误校验	
01	03	2	41	24	XX	
十六进制数 4124 表示的十进制整数为 16676，错误校验值要根据传输方式而定。						

主机请求： 设备地址、功能码、数据（N 个 8bit）、CRC

例：01 号读 3 个采集的数据（数据帧 2 个字节）UA、UB、UC。地址分别为：
UA=0025H、UB=0026H、UC=0027H

01H 03H 00H 25H 00H 03H 14H 00H

从机响应： 设备地址、功能码、数据数目、数据、CRC

例：UA=082CH UC=082AH UD=082CH

01H 03H 06H 08H 2CH 08H 2AH 08H 2CH 94H 4EH

表 1 ModBus 功能码

功能码	名称	作用
01	读取线圈状态	取得一组逻辑线圈的当前状态（ON/OFF)
02	读取输入状态	取得一组开关输入的当前状态（ON/OFF)
03	读取保持寄存器	在一个或多个保持寄存器中取得当前的二进制值
04	读取输入寄存器	在一个或多个输入寄存器中取得当前的二进制值
05	强置单线圈	强置一个逻辑线圈的通断状态
06	预置单寄存器	把具体二进值装入一个保持寄存器
07	读取异常状态	取得 8 个内部线圈的通断状态，这 8 个线圈的地址由控制器决定，用户逻辑可以将这些线圈定义，以说明从机状态，短报文适宜于迅速读取状态
08	回送诊断校验	把诊断校验报文送从机，以对通信处理进行评鉴
09	编程（只用于 484）	使主机模拟编程器作用，修改 PC 从机逻辑
10	控询（只用于 484）	可使主机与一台正在执行长程序任务从机通信，探询该从机是否已完成其操作任务，仅在含有功能码 9 的报文发送后，本功能码才发送
11	读取事件计数	可使主机发出单询问，并随即判定操作是否成功，尤其是该命令或其他应答产生通信错误时
12	读取通信事件记录	可是主机检索每台从机的 ModBus 事务处理通信事件记录。如果某项事务处理完成，记录会给出有关错误
13	编程（184/384 484 584）	可使主机模拟编程器功能修改 PC 从机逻辑
14	探询（184/384 484 584）	可使主机与正在执行任务的从机通信，定期控询该从机是否已完成其程序操作，仅在含有功能 13 的报文发送后，本功能码才得发送
15	强置多线圈	强置一串连续逻辑线圈的通断
16	预置多寄存器	把具体的二进制值装入一串连续的保持寄存器
17	报告从机标识	可使主机判断编址从机的类型及该从机运行指示灯的状态
18	（884 和 MICRO 84）	可使主机模拟编程功能，修改 PC 状态逻辑
19	重置通信链路	发生非可修改错误后，是从机复位于已知状态，可重置顺序字

		节
20	读取通用参数（584L）	显示扩展存储器文件中的数据信息
21	写入通用参数（584L）	把通用参数写入扩展存储文件，或修改之
22～64	保留作扩展功能备用	
65～72	保留以备用户功能所用	留作用户功能的扩展编码
73～119	非法功能	
120～127	保留	留作内部作用
128～255	保留	用于异常应答

表 2 ModBus 功能码与数据类型对应表

代码	功能	数据类型
01	读	位
02	读	位
03	读	整型、字符型、状态字、浮点型
04	读	整型、状态字、浮点型
05	写	位
06	写	整型、字符型、状态字、浮点型
08	N/A	重复“回路反馈”信息
15	写	位
16	写	整型、字符型、状态字、浮点型
17	读	字符型

通讯信息传输过程：

当通讯命令由发送设备（主机）发送至接收设备（从机）时，符合相应地址码的从机接收通讯命令，并根据功能码及相关要求读取信息，如果 CRC 校验无误，则执行相应的任务，然后把执行结果（数据）返送给主机。返回的信息中包括地址码、功能码、执行后的数据以及 CRC 校验码。如果 CRC 校验出错就不返回任何信息。

1.1 地址码：

地址码是每次通讯信息帧的第一字节（8 位），从 0 到 255。这个字节表明由用户设置地址的从机将接收由主机发送来的信息。每个从机都必须有唯一的地址码，并且只有符合地址码的从机才能响应回送信息。当从机回送信息时，回送数据均以各自的地址码开始。主机发送的地址码表明将发送到的从机地址，而从机返回的地址码表明回送的从机地址。相应的地址码表明该信息来自于何处。

1.2 功能码：

是每次通讯信息帧传送的第二个字节。ModBus 通讯规约可定义的功能码为 1 到 127。PDM 系列仪表/变送器仅用到其中的一部分功能码。作为主机请求发送，通过功能码告诉从机应执行什么动作。作为从机响应，从机返回的功能码与从主机发送来的功能码一样，并表明从机已响应主机并且已进行相关的操作。

1.3 数据区：

数据区包括需要由从机返送何种信息或执行什么动作。这些信息可以是数据（如：开关量输入/输出、模拟量输入/输出、寄存器等等）、参考地址等。例如，主机通过功能码 03 告诉从机返回寄存器的值（包含要读取寄存器的起始地址及读取寄存器的长度），则返回的数据包括寄存器的数据长度及数据内容。对于不同的从机，地址和数据信息都不相同（应给出通讯信息表）。

功能码“01”：读 1 路或多路开关量输出状态

例如：主机要读取地址为 01，开关量 DO1，DO2 的输出状态。
从机（PDM）数据寄存器的地址和数据为：

起始位地址	DO 寄存器数据(16 进制)	备 注
0000	2	DO2 输出状态为“1”，DO1 输出状态为“0”

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	1	发送至地址为 01 的从机
功能码	1	1	读开关量输出状态
起始 BIT 位	2	0000	起始 BIT 位地址为 0000
读数据长度	2	0002	读取 2 路继电器输出状态位
CRC 码	2	BDCB	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：

从机响应	字节数	返回的信息	备 注
从机地址	1	01	来自从机 01
功能码	1	01	读开关量输出状态
数据长度	1	01	1 个字节（8 个 BIT 位）
DO 状态数据	1	02	DO 寄存器内容
CRC 码	2	D049	由主机计算得到 CRC 码

功能码“02”：读 1 路或多路开关量状态输入

例如：主机要读取地址为 01，开关量 DI1—DI4 的输入状态。
从机（PDM）数据寄存器的地址和数据为：

起始位地址	DI 寄存器数据(16 进制)	备 注
0000	0B	DI1/DI2/DI4 状态为“1”，DI3 状态为“0”

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	01	发送至地址为 01 的从机
功能码	1	02	读开关量输入状态
起始 BIT 位	2	0000	起始 BIT 位地址为 0000
读数据长度	2	0004	读取 4 路继电器输入状态位
CRC 码	2	79C9	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：

从机响应	字节数	返回的信息	备 注
从机地址	1	01	来自从机 01
功能码	1	02	读开关量输入状态
数据长度	1	01	1 个字节（8 个 BIT 位）
DI 状态数据	1	0B	DI 寄存器内容
CRC 码	2	E04F	由主机计算得到 CRC 码

功能码“03”：读多路寄存器输入

例如：主机要读取地址为 01，起始地址为 0116 的 3 个从机寄存器数据。
从机（PDM）数据寄存器的地址和数据为：

寄存器地址	寄存器数据（16 进制）	对应 PDM 电量
0116	1784	UA
0117	1780	UB
0118	178A	UC

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	01	发送至地址为 01 的从机
功能码	1	03	读取寄存器
起始地址	2	0116	起始地址为 0116
读数据长度	3	0003	读取 3 个寄存器（共 6 个字节）
CRC 码	2	E5F3	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：

从机响应	字节数	返回的信息	备 注
从机地址	1	01	来自从机 01
功能码	1	03	读取寄存器
读取字	1	06	3 个寄存器共 6 个字节
寄存器数据 1	2	1784	地址为 0116 内存的内容
寄存器数据 2	2	1780	地址为 0117 内存的内容
寄存器数据 3	2	178A	地址为 0118 内存的内容
CRC 码	2	5847	由从机计算得到 CRC 码

功能码“05”：写 1 路开关量输出（“遥控”）

例 1：开关量输出点 DO1，其当前状态为“分”，主机要控制该路继电器“合”。

控制命令为：
“FF00”为控制继电器“合”；
“0000”为控制继电器“分”；

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	01	发送至地址为 01 的从机
功能码	1	05	写开关量输出状态
输出 BIT 位	2	0000	对应输出继电器 BIT 位（DO1）
控制命令	2	FF00	控制该路继电器输出为“合”状态位
CRC 码	2	8C3A	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：
与主机发送的报文格式及数据内容完全相同。

例 2：开关量输出点 DO2，其当前状态为“合”，主机要控制该路继电器“分”。

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	01	发送至地址为 01 的从机
功能码	1	05	写开关量输出状态
输出 BIT 位	2	0001	对应输出继电器 BIT 位（DO2）
控制命令	2	0000	控制该路继电器输出为“合”状态位
CRC 码	2	9C0A	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：

与主机发送的报文格式及数据内容完全相同。

功能码“06”：写单路寄存器

例如：主机要把数据 07D0，保存到地址为 002C 的从机寄存器中去（从机地址码为 01）。
通讯数据保存结束后，地址为 002C 的 PDM 表原存储信息为：

地址	原来存储数据（16 进制）
002C	04B0

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	01	发送至地址为 01 的从机
功能码	1	06	写单路寄存器
起始地址	2	002C	要写入的寄存器地址
写入数据	2	07D0	对应的新数据
CRC 码	2	4BAF	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：
与主机发送的报文格式及数据内容完全相同。

功能码“10”：写多路寄存器

主机利用这个功能码把多个数据保存到 PDM 表的数据存储器中去。Modbus 通讯规约中的寄存器指的是 16 位（即 2 字节），并且高位在前。这样 PDM 的存储器都是二个字节。由于 Modbus 通讯规约允许每次最多保存 60 个寄存器，因此 PDM 一次也最多允许保存 60 个数据寄存器。
例如：主机要把 0064，0010 保存到地址为 002C，002D 的从机寄存器中去（从机地址码为 01）。通讯数据保存结束后，地址为 002C/002D 的 PDM 表内存储信息为：

地址	原来存储数据（16 进制）
002C	04B0
002D	1388

主机发送的报文格式：

主机发送	字节数	发送的信息	备 注
从机地址	1	01	发送至地址为 01 的从机
功能码	1	10	写多路寄存器
起始地址	2	002C	要写入的寄存器的起始地址
保存数据字长度	2	0002	保存数据的字长度（共 2 字）
保存数据字节长	1	04	保存数据的字节长度（共 4 字节）
保存数据 1	2	04B0	数据地址 002C
保存数据 2	2	1388	数据地址 002D
CRC 码	2	FC63	由主机计算得到 CRC 码

从机（PDM）响应返回的报文格式：

从机响应	字节数	返回的信息	备 注
从机地址	1	01	来自从机 01
功能码	1	10	写多路寄存器
起始地址	2	002C	起始地址为 002C
保存数据字长度	2	0002	保存 2 个字长度的数据
CRC 码	2	8001	由从机计算得到 CRC 码

通讯错误信息及数据的处理：

当 PDM 表检测到除了 CRC 码出错以外的错误时，必须向主机回送信息，功能码的最高位置为 1，即从机返送给主机的功能码是在主机发送的功能码的基础上加 128 。以下的这些代码表明有意外的错误发生。

PDM 从主机接收到的信息如有 CRC 错误，则将被 PDM 表忽略。

PDM 返送的错误码的格式如下（CRC 码除外）：

地址码： 1 字节

功能码： 1 字节（最高位为 1）

错误码： 1 字节

CRC 码：2 字节。

PDM 响应回送如下错误码：

81．非法的功能码。

接收到的功能码 PDM 表不支持。

82．非法的数据位置。

指定的数据位置超出 PDM 表的范围。

83．非法的数据值。

接收到主机发送的数据值超出 PDM 相应地址的数据范围。