# MODBUS-RTU通讯协议

MODBUS-RTU通讯协议采用主从应答方式(半双工)，主机发出指令寻址某一从机，被寻址的从机响应并返回应答信息。

## 一、通讯格式

### 1.1 传输格式

信息传输为异步方式，并以字节为单位(LSB先)，在主机和从机之间传递的通讯信息为11位的字格式。

有奇偶校验的传输序列：1个起始位、8个数据位、1个校验位、1个停止位。


无奇偶校验的传输序列：1个起始位、8个数据位、2个停止位。


### 1.2 帧格式

一个新的通讯信息帧开始之前，通讯总线应存在不小于3.5字节的间歇时间，通讯开始之后，每两个字节之间应不大于1.5字节的间歇时间。

| 开　始 | 地址码 | 功能码 | 数据区 | CRC校验码低字节 | CRC校验码高字节 | 结　束 |
|---|---|---|---|---|---|---|
| ≥3.5字节间歇时间 | 1字节 | 1字节 | n字节 | 1字节 | 1字节 | ≥3.5字节间歇时间 |

## 二、通讯信息帧说明

主机寻址某一从机时，与主机发送的地址码相符的从机接收通讯命令，如果CRC校验无误，则执行相应的操作，然后把执行结果(数据)回送给主机，否则不返回任何信息。

### 2.1 地址码

地址码是通讯信息帧的第1个字节，从1到247。每个从机应该有总线内唯一的地址码，只有与主机发送的地址码相符的从机才能响应并回送信息。从机支持广播地址0。

### 2.2 功能码

功能码是通讯信息帧的第2个字节。主机寻址某一从机时，通过功能码告诉从机执行什么操作。从机返回的功能码与主机发送的功能码一致表明从机已正确执行了相关操作。从机支持以下功能码：

| 功能码(16进制) | 定　义 | 说　明 |
|---|---|---|
| 01H | 读DO状态 | 获得仪表内部继电器的通断状态(ON/OFF) |
| 02H | 读DI状态 | 获得仪表外部开关的通断状态(ON/OFF) |
| 03H/04H | 读寄存器 | 获得n个(n≥1)连续的寄存器的数据 |
| 05H | 控制DO | 改变仪表内部一个继电器的通断状态(ON/OFF) |
| 06H | 写单个寄存器 | 改变一个寄存器的数据 |
| 10H | 写多个连续的寄存器 | 改变n个(n≥1)连续的寄存器的数据 |

### 2.3 数据区

数据区的长度和内容随功能码不同而不同，用于主机和从机以读写寄存器的方式进行数据交换。产品使用说明书中给出了具体的通讯信息表。

### 2.4 CRC校验码

CRC校验码高字节是通讯信息帧的最后一个字节。

CRC校验码由主机计算，放置于发送信息帧的尾部。从机再重新计算接收到信息的CRC，比较计算得到的CRC与接收到的CRC是否一致，如果不一致则表明出错。CRC计算只用到了8个数据位，计算方法如下：

①预置1个16位的寄存器为十六进制FFFF(即全为1)，称此寄存器为CRC寄存器

②把第一个8位二进制数据(通讯信息帧的第1个字节)与16位CRC寄存器的低8位相异或，结果放于CRC寄存器

③把CRC寄存器的内容右移一位(朝低位)并用0填补最高位，检查右移后的移出位

④如果移出位为0：重复第③步(再次右移一位)；

如果移出位为1：CRC寄存器与多项式A001(1010 0000 0000 0001)进行异或

⑤重复步骤③和④，直到右移8次，这样整个8位数据全部进行了处理

⑥重复步骤②到步骤⑤，进行通讯信息帧下一个字节的处理

⑦将该通讯信息帧所有字节(不包括CRC校验码低、高字节)按上述步骤计算完成后，CRC寄存器内容即为CRC校验码。

## 三、功能码说明

### 3.1 功能码01H：读DO状态（1=ON，0=OFF）

例1：主机要读取从机地址为01H，起始地址为00H的4个继电器的通断状态　主机发送：01 01 00 00 00 04 3D C9

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 01H |
| 起始地址 | 高字节 | 00H |
| | 低字节 | 00H |
| 数量 | 高字节 | 00H |
| | 低字节 | 04H |
| CRC校验码 | 低字节 | 3DH |
| | 高字节 | C9H |

如果从机地址为01H，起始地址为00H的4个继电器状态分别为OFF、OFF、ON、ON　从机返回：01 01 01 0C 51 8D

| 从机返回 | | 返回的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 01H |
| 返回的数据字节数 | | 01H |
| 返回的数据 | | 0CH |
| CRC校验码 | 低字节 | 51H |
| | 高字节 | 8DH |

返回的数据0CH：bit3～bit0分别对应03H～00H 4个继电器的通断状态。

例2：主机要读取从机地址为01H，地址为02H的1个继电器的通断状态　主机发送：01 01 00 02 00 01 5C 0A

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 01H |
| 起始地址 | 高字节 | 00H |
| | 低字节 | 02H |
| 数量 | 高字节 | 00H |
| | 低字节 | 01H |
| CRC校验码 | 低字节 | 5CH |
| | 高字节 | 0AH |

如果从机地址为01H，地址为02H的继电器状态为ON，从机返回：01 01 01 01 90 48

| 从机返回 | | 返回的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 01H |
| 返回的数据字节数 | | 01H |
| 返回的数据 | | 01H |
| CRC校验码 | 低字节 | 90H |
| | 高字节 | 48H |

返回的数据01H：bit0对应02H 继电器的通断状态。

### 3.2 功能码02H：读DI状态（1=ON，0=OFF）

例1：主机要读取从机地址为01H，起始地址为00H的4个外部开关的通断状态　主机发送：01 02 00 00 00 04 79 C9

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 02H |
| 起始地址 | 高字节 | 00H |
| | 低字节 | 00H |
| 数量 | 高字节 | 00H |
| | 低字节 | 04H |
| CRC校验码 | 低字节 | 79H |
| | 高字节 | C9H |

如果从机地址为01H，起始地址为00H的4个外部开关状态分别为OFF、OFF、ON、ON　从机返回：01 02 01 0C A1 8D

| 从机返回 | | 返回的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 02H |
| 返回的数据字节数 | | 01H |
| 返回的数据 | | 0CH |
| CRC校验码 | 低字节 | A1H |
| | 高字节 | 8DH |

返回的数据0CH：bit3～bit0分别对应03H～00H 4个外部开关通断状态。

例2：主机要读取从机地址为01H，地址为02H的1个外部开关的通断状态　主机发送：01 02 00 02 00 01 18 0A

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 02H |
| 起始地址 | 高字节 | 00H |
| | 低字节 | 02H |
| 数量 | 高字节 | 00H |
| | 低字节 | 01H |
| CRC校验码 | 低字节 | 18H |
| | 高字节 | 0AH |

如果从机地址为01H，地址为02H的开关状态为ON，从机返回：01 02 01 01 60 48

| 从机返回 | | 返回的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 02H |
| 返回的数据字节数 | | 01H |
| 返回的数据 | | 01H |
| CRC校验码 | 低字节 | 60H |
| | 高字节 | 48H |

返回的数据01H：bit0对应02H 外部开关的通断状态。

### 3.3 功能码03H/04H：读寄存器

例1：主机要读取从机地址为01H，地址为1DH的1个寄存器数据。主机发送：

03H功能码：01 03 00 1D 00 01 14 0C

04H功能码：01 04 00 1D 00 01 A1 CC

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 03H/04H |
| 起始寄存器地址 | 高字节 | 00H |
| | 低字节 | 1DH |
| 寄存器数量 | 高字节 | 00H |
| | 低字节 | 01H |
| CRC校验码 | 低字节 | 14H/A1H |
| | 高字节 | 0CH/CCH |

如果从机地址为01H，地址为1DH的寄存器数据为000AH，从机返回：

03H功能码：01 03 02 00 0A 38 43

04H功能码：01 04 02 00 0A 39 37

| 从机返回 | | 返回的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 03H/04H |
| 返回的数据字节数 | | 02H |
| 寄存器数据 | 高字节 | 00H |
| | 低字节 | 0AH |
| CRC校验码 | 低字节 | 38H/39H |
| | 高字节 | 43H/37H |

例2：主机要读取从机地址为01H，起始寄存器地址为25H的3个寄存器数据。主机发送：

03H功能码：01 03 00 25 00 03 14 00

04H功能码：01 04 00 25 00 03 A1 C0

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 03H/04H |
| 起始寄存器地址 | 高字节 | 00H |
| | 低字节 | 25H |
| 寄存器数量 | 高字节 | 00H |
| | 低字节 | 03H |
| CRC校验码 | 低字节 | 14H/A1H |
| | 高字节 | 00H/C0H |

如果从机地址为01H，地址为25H、26H、27H的3个寄存器的数据分别为0898H、0896H、089CH。从机返回：

03H功能码：01 03 06 08 98 08 96 08 9C E4 04

04H功能码：01 04 06 08 98 08 96 08 9C A5 E2

| 从机返回 | | 返回的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 03H/04H |
| 返回的数据字节数 | | 06H |
| 25H寄存器数据 | 高字节 | 08H |
| | 低字节 | 98H |
| 26H寄存器数据 | 高字节 | 08H |
| | 低字节 | 96H |
| 27H寄存器数据 | 高字节 | 08H |
| | 低字节 | 9CH |
| CRC校验码 | 低字节 | E4H/A5H |
| | 高字节 | 04H/E2H |

### 3.4 功能码05H：控制DO（ON=FF00H，OFF=0000H）

例如：主机要将从机地址为01H，地址为01H的继电器切换到接通/断开状态。主机发送：

接通：01 05 00 01 FF 00 DD FA

断开：01 05 00 01 00 00 9C 0A

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 05H |
| 地址 | 高字节 | 00H |
| | 低字节 | 01H |
| 发送的数据 | 高字节 | FFH/00H |
| | 低字节 | 00H/00H |
| CRC校验码 | 低字节 | DDH/9CH |
| | 高字节 | FAH/0AH |

如果地址为01H的从机正确执行了相关操作，则返回的数据与主机发送数据完全一致。

### 3.5 功能码06H：写单个寄存器

例如：主机要将从机地址为01H，地址为03H的寄存器的值改为0028H。

主机发送：01 06 00 03 00 28 79 D4

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 06H |
| 寄存器地址 | 高字节 | 00H |
| | 低字节 | 03H |
| 写入的数据 | 高字节 | 00H |
| | 低字节 | 28H |
| CRC校验码 | 低字节 | 79H |
| | 高字节 | D4H |

如果地址为01H的从机正确执行了相关操作，则返回的数据与主机发送数据完全一致。

### 3.6 功能码10H：写多个连续的寄存器

例1：主机要将从机地址为01H，地址为03H的1个寄存器的值改为0028H。

主机发送：01 10 00 03 00 01 02 00 28 A6 7D

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 10H |
| 起始寄存器地址 | 高字节 | 00H |
| | 低字节 | 03H |
| 寄存器数量 | 高字节 | 00H |
| | 低字节 | 01H |
| 写入的数据字节数 | | 02H |
| 03H寄存器写入的数据 | 高字节 | 00H |
| | 低字节 | 28H |
| CRC校验码 | 低字节 | A6H |
| | 高字节 | 7DH |

如果地址为01H的从机正确执行了相关操作，

从机返回：01 10 00 03 00 01 F1 C9

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 10H |
| 起始寄存器地址 | 高字节 | 00H |
| | 低字节 | 03H |
| 寄存器数量 | 高字节 | 00H |
| | 低字节 | 01H |
| CRC校验码 | 低字节 | F1H |
| | 高字节 | C9H |

例2：主机要把数据0000H、1388H、000AH写入到从机地址为01H，起始寄存器地址为09H的3个寄存器中。

主机发送：01 10 00 09 00 03 06 00 00 13 88 00 0A 32 06

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 10H |
| 起始寄存器地址 | 高字节 | 00H |
| | 低字节 | 09H |
| 寄存器数量 | 高字节 | 00H |
| | 低字节 | 03H |
| 写入的数据字节数 | | 06H |
| 09H寄存器写入的数据 | 高字节 | 00H |
| | 低字节 | 00H |
| 0AH寄存器写入的数据 | 高字节 | 13H |
| | 低字节 | 88H |
| 0BH寄存器写入的数据 | 高字节 | 00H |
| | 低字节 | 0AH |
| CRC校验码 | 低字节 | 32H |
| | 高字节 | 06H |

如果地址为01H的从机正确执行了相关操作，

从机返回：01 10 00 09 00 03 50 0A

| 主机发送 | | 发送的信息 |
|---|---|---|
| 地址码 | | 01H |
| 功能码 | | 10H |
| 起始寄存器地址 | 高字节 | 00H |
| | 低字节 | 09H |
| 寄存器数量 | 高字节 | 00H |
| | 低字节 | 03H |
| CRC校验码 | 低字节 | 50H |
| | 高字节 | 0AH |

## 四、出错处理

当从机检测到了除CRC校验码错误以外的其它错误时，应向主机回送信息。从机返回的功能码最高位为1(即从机返回的功能码是主机发送的功能码+128)，表明本次通讯存在错误。

### 4.1 从机返回的信息帧格式

| 开　始 | 地址码 | 功能码 | 错误码 | CRC校验码低字节 | CRC校验码高字节 | 结　束 |
|---|---|---|---|---|---|---|
| ≥3.5字节间歇时间 | 1字节 | 1字节 | 1字节 | 1字节 | 1字节 | ≥3.5字节间歇时间 |

### 4.2 错误码说明

| 错误码 | 说　明 |
|---|---|
| 01H | 接收到的功能码从机不支持 |
| 02H | 接收到的寄存器地址超范围或寄存器地址+寄存器数量超范围 |
| 03H | 接收到的寄存器数量超范围或写入的数据超范围 |
| 04H | 因写入数据超范围或对用于报警的继电器进行写入而导致写入失败 |