# V80 和 PPC 系列可编程控制器

# MODBUS 通讯协议

# （Ver1.2）


德维森科技(深圳)有限公司

地址：深圳市南山区高新区科技南 12 路中电照明中心北二楼
邮编：518057
电话：0755-26715433，0755-26715552
传真：0755-26715422
网址：http://www.techwayson.com

# 目　　录

# 1 MODBUS 协议

该协议定义了 ModBus 总线 MASTER（主站）与 SLAVE（从站）之间的通讯报文格式，对于主站来说，MODBUS 协议是联系 PLC 的接口，而且所有的通讯都是“透明的”。

MODBUS 协议是工业最常用的 PLC 通信协议 包含 RTU 及 ASC II 两种 格式，两种格式的报文各字段解释是相同的。他们之最大的差别他们执行错误核对的方式与字符的格式。

## 1.1 ASC II 结构

在 ASC II 的传输模式中，其格式中各栏的使用如下表所示:

以引号表示帧的开始。

以回车(CARRIAGE RETURN)和 LF (LINE FEED)来表示一个帧的结束。

LF 同时也用作同步信号，以表示传送站已准备好去接收一个立即的响应。

| BEF OF FRAME | ADDRESS | FUNCTION | DATA | ERROR CHECK | EOF | READY TO RECRESP |
|---|---|---|---|---|---|---|
| : | 2-CHAR 16-BITS | 2-CHAR 16-BITS | N*2 CHAR N* 16-BITS | 2-CHAR 16-BITS | CR | LF |

CHAR=CHARACTER: 1 CHARACTER=7 DATA BITS， 1 START BIT， 1 OR 2 STOP BITS AND OPTIONALLY-1 PARITY BIT

图 1-1 ASC II 报文帧格式

## 1.2 REMOTE TERMINAL UNIT (RTU)

在 RTU 模式存在帧同步时间。(以表示一个帧的起始和结束)，接收站监视连续 2 个字符之间的时间间隔，如发现总线空闲超过 4 个半字符时间则认为一个帧已结束，同时认为下一个字符为下一帧的帧地址。

| T1T2T3 | ADDRESS | FUNCTION | DATA | CHECK | T1T2T3 |
|---|---|---|---|---|---|
| | 8-BITS | 8-BITS | N*8-BITS | 2*8-BITS | |

图 1-2 RTU 报文帧格式

## 1.3 站地址

地址可由 8-BITS (RTU)或 2 个字符所组成，这些位指示出那个从站(使用者寻址)应去接收由主站所传送来的报文。

每个从站必须指定一个唯一的站地址，而唯有报文地址与该从站的地址相同时，该从站

才会响应主站的通信。当从站送出应答报文后，从站的地址告诉主站是那一个从站正在通讯中。而广播报文，它的地址是零。所有的从站将“零”解释成去读和动作此报文的指令，但接收到报文的从站都不会应答主站。

## 1.4 功能码

功能码指示被寻址到的从站应该作什么动作，功能码的高位如果从站装置设定为某值，以告诉主站，一个不正常的响应正在传送给它，如果从站应答的功能码与主站下传的功能码一致.则表示所传送的是一个应答或响应的报文。下表列出 MODBUS 的功能码。

表 1-1 功能码

| 码 | 意义 |
|---|---|
| 01 | 读线圈状态(READ COIL STATUS) |
| 02 | 读输入接点（READ INPUT STATUS） |
| 03 | 读保持型寄存器(READ HOLDING REGISTER) |
| 04 | 读输入型寄存器(READ INPUT REGISTER) |
| 05 | 写单线圈(FORCE SINGLE COIL) |
| 06 | 写单寄存器(PRESET SINGLE REGISTER) |
| 15 | 写多线圈(FORCE MULTIPLE COILS) |
| 16 | 写多寄存器(PRESET MULTIPLE REGISTERS) |

## 1.5 数据区

数据区包含从站欲执行特定功能时所需要的信息或者包含从站被询问后所应答给主站的信息。这些信息包含地址偏移、长度、数据。例如:从从站读取寄存器的功能码，去读的寄存器的基地址及读多少个数据。

## 1.6 校验码

校验码可让主站或从站去检查传输过程中是否有错误发生，有时候因为噪声或其它的干扰会使传送或接收中的资料出错，而校验可以使主站或从站不对错误的报文作动作，所以校验可以增加 MODBUS 系统的安全性及效率。

在校验码中，对于 ASC II 模式采用的是 LRC (LONG ITUDINAL REDUNDANCE CHECK)的侦错法，在 RTU 模式则使用 CRC-16 校验码。

如果询问或响应的报文可以用中文表示的话，则报文中的 4 个字段就会如下图所示。

(NOTE:传送的顺序是——站地址 功能码 数据区 校验码)

MODBUS 的询问/应答报文的内容

| 校验 | 资料 | 功能码 | 地址 |
|---|---|---|---|
| 整个帧的校验码 | 数据及扩展命令 | 命令 | 对从站 N 的询问 |

MASTER
主站

SLAVE
从站

| 地址 | 功能码 | 资料 | 校验 |
|---|---|---|---|
| 从从站 N 所传的应答 | 重复主站的命令 | 应答的数据 | 整个帧的校验 |

# 2 通讯功能

在功能码 1 到 6， 15 和 16 的报文会指出 MODBUS 上的那一块特定的数据区域会被寻址到，例如功能码 1 ，5 及 15 会指向线圈 COIL (0XXXX)，功能码 2 指向输入接点（1XXXX），功能 3， 6 及 16 参考到保持型寄存器(HOLDING REGISTER) (4XXXX)，功能码 4 指向输入接点（3XXXX）。所有的参考地址都是以相对于零来做参考点，例如 COIL 00127 是以 0126 来被参考到的(0126 decimal)=007E(hex)，在 MODBUS 的格式里所有的数字都是以十六进制的方式来表示的。

在本章中所举的例子都将以 RTU 模式为例，读者可以利用以下的方法来编写自己的协议来与 PLC 通信或联网。

下示的例子是“读保持型寄存器” 40108～40110 (M-BUS 从站的站地址是 06)，报文分别以 RTU 或 ASC II 模式来表示，将会如下图所显示:

主站发送：

| 报 文 | | RTU（bit） | | |
|---|---|---|---|---|
| 帧头 | | 无 | | |
| 站地址 | | 0000 | 0110 | 06 |
| 功能码 | | 0000 | 0011 | 03 |
| 寄存器起始地址：高字节 | | 0000 | 0000 | 00 |
| | 低字节 | 0110 | 1011 | 6B |
| 读寄存器的数目:高字节 | | 0000 | 0000 | 00 |
| | 低字节 | 0000 | 0011 | 03 |
| 校验码 | 高字节 | 0111 | 0101 | 75 |
| | 低字节 | 1010 | 0000 | A0 |
| 帧尾 | | 无 | | |
| | | 共 8 字节 | | |

应答:

| 报　文 | | RTU（bit） | | |
|---|---|---|---|---|
| 帧头 | | 无 | | |
| 站地址 | | 0000 | 0110 | 06 |
| 功能码 | | 0000 | 0011 | 03 |
| 数据长度: | | 0000 | 0110 | 06 |
| 数据 | 高字节 | 0000 | 0010 | 00 |
| 数据 | 低字节 | 0110 | 1011 | 63 |
| 数据 | 高字节 | 0000 | 0010 | 00 |
| 数据 | 低字节 | 0110 | 1011 | 63 |
| 数据 | 高字节 | 0000 | 0000 | 00 |
| 数据 | 低字节 | 0110 | 0011 | 63 |
| CRC 校验 | 高字节 | 0111 | 0011 | 73 |
| CRC 校验 | 低字节 | 0111 | 1010 | 7A |
| 帧尾 | | 无 | | |
| | | 共 11 字节 | | |

## 2.1 读取线圈状态(功能码 01)-READ OUTPUT 0XXXX STATUS

1. 询问

此功能让主站可以从从站中读取线圈的(LOGIC COIL)开/关的状态，广播模式并不支持该功能码。每次询问最多可以读取到 1024 个线圈，不过，有许多的从站会根据系统的性能要求，而限制在此最大量以下。

特别注意的一点就是线圈的起始号码与实际的对应，因为 PLC 的线圈是从 1 起始的，而 ModBus 通信协议中定义的线圈是从 0 开始的，因此 PLC 的 0001 线圈对应的是 ModBus 中的 0000,依此类推 图 1-2-1 是此功能的例子,读取的是 17 号从站上的 COIL 00020 到 00056 的状态:

| ADDR | FUNC | DATA START PT HI | DATA START PT LO | DATA #OF PTS HI | DATA #OF PTS HI | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 01 | 00 | 13 | 00 | 25 | 0E | 84 |

图 1-2-1 读输出状态询问报文

2. 响应

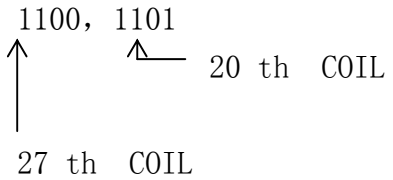
在图 5~3 显示的就是从站对询问所作的响应报文，每个位表示一个线圈。响应的报文包含有从站的站地址 功能码 资料字符的数目 资料字符及校验码，COIL 的位如果是 1 的话就代表是 ON，对于那些 COIL 的数目未达到 8 的倍数的部分，在高位的尾端便填零。

比方说读取的是从 0002 开始地址的 3 个位，而 0001~0016 的数值为 0101 0110，则上传

的数据为 0000 0011。

线圈的排列顺序如下图所示:

COIL 20 到 27 的状态是 CD (HEX)=1100，1101(BINARY)，此表示 COIL 的次序是从右到左，其对应如右




| ADDR | FUNC | BYTE COUNT | DATA COIL STATUS 20-27 | DATA COIL STATUS 28-35 | DATA COIL STATUS 36-43 | DATA COIL STATUS 44-51 | DATA COIL STATUS 52-56 | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|---|---|
| 11 | 01 | 05 | CD | 6B | B2 | 0E | 1B | 45 | E6 |

图 1-2-2 读输出状态响应报文

从上图可知 COIL 27，26，23，22 及 20 都是 ON 的状态，而 52 到 59 这 8 位当中的最左三位都被设为零。

## 2.2 读保持型寄存器(功能码 03) READ OUTPUT 4XXXX REGISTER

1.询问:

此功能允许主站寻址从站中的保持型寄存器(HOLDING REGISTER)的 16 进制内容 这些寄存器可用来储存有关的定时器或计数器的数值。每次询问可以寻址最大 125 个寄存器，这些寄存器从零开始算起，40001=ZERO，40002=ONE，....)

广播模式在此功能是不允许的。

以下的例子是从第 17 号从站中读取从 40108 到 40110 的寄存器的内容。

| ADDR | FUNC | DATA START REG HI | DATA START REG LO | DATA #OF REGS HI | DATA #OF REGS LO | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 03 | 00 | 6B | 00 | 03 | 76 | 87 |

图 1-2-3 读输出寄存器询问报文

2.响应

被寻址到的从站所响应的报文包括功能码及地址及数据长度，数据长度包含 2 个字节以描述从站应答的数据字节长度。

在下列中显出 40108 到 40110 的缓存器各拥有 555，0 及 100 的十进制值。

| ADDR | FUNC | BYTE COUNT | DATA OUTPUT REG HI 40108 | DATA OUTPUT REG LO 40108 | DATA OUTPUT REG HI 40109 | DATA OUTPUT REG LO 40109 | DATA OUTPUT REG HI 40110 | DATA OUTPUT REG LO 40110 | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 03 | 06 | 02 | 2B | 00 | 00 | 00 | 64 | C8 | BA |

图 1-2-4 读输出寄存器响应报文

## 2.3 写单一线圈(功能码 05)FORCE SINGLE COIL 0XXX

1.询问:

此功能可写单一线圈的开或关。在控制器内的任何线圈都能够被强制成 ON 或 OFF 的状态。因为控制器是主动地在扫描，如果同一线圈 PLC 与主站都进行写，则双方都可以进行控制。

线圈的号数也是从零算起(COIL 0001=0，COIL 0002=1....)，如果给定为零则会使 COIL OFF 掉，其余的值都是不合法的，所以也不会影响到 COIL 的状态。

当站地址被定为零(广播模式)，则会使所有的从站去会对同一 COIL 进行修改。

下面的例子是使从站 17 的 COIL 00173 变成 ON 的状态。

| ADDR | FUNC | DATA COIL # HI | DATA COIL # LO | DATA ON OFF IND | DATA ON OFF IND | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 05 | 00 | AC | FF | 00 | 4E | 8B |

图 1-2-5 写单一线圈询问报文

写 COIL 成功后重传接收到的报文。

| ADDR | FUNC | DATA COI I # HI | DATA COI I # LO | DATA ON OFF IND | DATA ON OFF IND | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 05 | 00 | AC | FF | 00 | 4E | 8B |

图 1-2-6 写单一线圈应答报文

## 2.4 写一个寄存器(功能码 06)-PRESET SINGLE REGISTER 4XXXX

1.询问:

此功能码允许使用者去更改一个保持型寄存器的内容，在控制器内的任何一个寄存器都能够应用这个报文来更改它的内容，虽然如此，因为控制器是主动扫描的，所以保持型寄存器不光被主站驱动，也有可能被 PLC 驱动，这需要用户自行回避多驱动的问题。这些值可以二进制的方式表示，其最大可达到控制器的最大容量，而不用的高字节位(HIGH ORDER BITS)必须设定成零。

| ADDR | FUNC | DATA REG #40136 HI | DATA REG #40136 LO | DATA VALUE HI | DATA VALUE LO | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 06 | 00 | 87 | 03 | 9E | BA | 2B |

图 1-2-7 设定寄存器询问报文

2.响应:

写寄存器成功后，从站重传接收到的报文。

| ADDR | FUNC | DATA REG 40136 HI | DATA REG 40136 LO | DATA VALUE | DATA VALUE | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 06 | 00 | 87 | 03 | 9E | BA | 2B |

图 1-2-8 设定寄存器应答报文

## 2.5 写多个线圈(功能码 15)-FORCE MULTIPLE COILS 0XXXX

1.询问:

此报文写多个线圈的状态 在控制器内的线圈都能够被强制成 ON 或 OFF 的状态，由于控制器一直主动地在扫描，所以除非 COIL 被强制，否则控制器也能够更改线圈的状态。

写的多个线圈的值包含在数据中，每一个位代表一个 COIL 的 ON 或 OFF，0 代表 OFF，1 代表 ON。

下例中，从开始地址 20(13HEX)起，有 10 个线圈被强制状态，数据域的 CD=1100，1101 和 00=0000，0000 表线圈 27，26，23，22 和 20 都被强制成 ON 的状态。

| ADDR | FUNC | HI ADDR | LO ADDR | QUANTITY | | BYTE CNT | DATA COIL STUS 20-27 | DATA COIL STUS 28-29 | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 0F | 00 | 13 | 00 | 0A | 02 | CD | 00 | 7E | CB |

图 1-2-9 写多线圈询问报文

2.响应:

正常的响应是从站站地址、功能码、起始地址及所写的 COIL 数目的回送 。

| ADDR | FUNC | HI ADDR | LO ADDR | QUANTITY | | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 0F | 00 | 13 | 00 | 0A | 26 | 99 |

图 1-2-10 写多线圈应答报文

## 2.6 写多个寄存器(功能码 16)PRESET MULTIPLE REGISTERS 4XXXX

1.询问:

任何的保持型寄存器(在控制器之内)都能够用这个报文来改变它的内容，但是控制器也能够同时更改它的保持型寄存器的内容，所以用户要自行回避多驱动的问题，最后不用的高位必须设定为零。

在广播模式中，所有的从控制器都将会把特定的内容加载到所指定的缓存器。

| ADDR | FUNC | HI ADDR | LO ADDR | QUANTITY | | BYTE CNT | HI DATA | LO DATA | HI DATA | LO DATA | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 10 | 00 | 87 | 00 | 02 | 04 | 00 | 0A | 01 | 02 | 4E | BA |

图 1-2-11 设定多缓存器询问报文

2.响应:

从站的应答是回传站地址、功能码、起始地址及所要写的寄存器的数据长度。

| ADDR | FUNC | HI ADDR | LO ADDR | QUANTITY | | CRC16 CHECK | |
|---|---|---|---|---|---|---|---|
| 11 | 10 | 00 | 87 | 00 | 02 | F3 | 71 |

图 1-2-12 设定多缓存器响应报文