西门子代理海南省海口市一级总代理PLC

产品名称	西门子代理海南省海口市一级总代理PLC
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子变频器:西门子触摸屏 西门子伺服电机:西门子PLC 西门子直流调速器:西门子电缆
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房
联系电话	18475208684 18475208684

产品详情

主要内容：

S7-200 PLC串口通讯概览

S7-200 PLC自由口通讯基础

S7-200 PLC自由口通讯指令

S7-200 PLC自由口通讯常问问题

（1）概览

S7-200串口通讯主要包括：1）Modbus—S7-200PLC与支持Modbus RTU协议的第三方设备通讯

RTU Master-Protocol（RTU主站协议）

RTU Slave-Protocol（RTU从站协议）

2）USS—S7-200PLC与SIEMENS驱动设备的通讯（如MM440等）3）自由口通讯—S7-200PLC与自由协议的第三方设备间的通讯

S7-200系列PLC可以方便地同计算机、打印机、变频器、扫描仪等其它的第三方设备进行无障碍通讯。

Modbus通讯和USS通讯是自由口通讯的特例。

对于S7-200系列的PLC而言，本体上存在着一个或两个485通讯接口，这种接口即可实现S7-200串口通讯的功能，这类串口既可以做编程和监控，也可以做自由口通讯。但在其运行自由口通讯程序时，无法对其进行监控。这是因为对于同一个口而言在同一个时刻只能支持一种协议，而编程与下载的协议对于S7-200PLC而言是PPI协议，所以一旦在程序运行过程中使得它做自由口通讯的状态则无法对其监控和下载。

下表是Modbus、USS以及自由口通讯的一些参数：

对于OSI七层模型而言，Modbus通讯、USS通讯和自由口通讯所处的位置可从上图中看到。

（2）自由口通讯

S7-200 CPU的通信口可以设置为自由口模式。选择自由口模式后，用户程序就可以完全控制通信端口的控制，通信协议也完全受用户程序控制。

所谓的自由口通讯，就是通讯协议是由用户自由定义的。

对于S7-200 PLC而言，基于本体自带的485端口的网络所应用的协议，除了PPI协议以外，其他都是自由口协议。例如USS协议、Modbus协议等等都是特定的自由口通讯协议。

1）自由口通讯硬件

西门子S7 -200系列PLC的自由口是基于RS485的硬件，采用正负两根信号线作为传输线路。两线间的电压差为+2V~6V表示逻辑"1"：两线间的电压差为-2V~-6V表示逻辑"0"。

西门子串口的插头是九针标准插头，其中各个针脚的定义在下表中得以体现，最重要的两根线是表中红线标出的3号脚和8号脚，也就是通常说的"3正8负"，其中3对应信号B，8对应信号A，其它的引脚可以完成一些额外的功能，比如24V直流电的供应，5V直流电的供应以及发送请求等。但是对于最基本的串口通讯而言，3脚和8脚两根线就足够了，所以下面将着重介绍这两根线的逻辑。

对于一根线上通过这两根线就可以完成如此复杂的通讯过程，它的传输逻辑一个是"1"一个是"0"，对于一个完整的报文帧而言，它的格式从下图中可以看出，首先包括一位起始位，中间是7或8位数据位，接下来是一位校验位或者没有校验位，最后附上一个停止位，从起始位到停止位是一个报文的全部内容，起始位在传输过程当中被永远定义为逻辑0，7或8位数据位0或1的逻辑状态完全取决于数据等于多少，校验位可有可无，如果有的话还分为奇校验和偶校验，它最终的逻辑是取决于前面数据位的组合关系，停止位固定为1。在整个报文帧之外的范围内，线上的状态为1，即为空闲状态。

2）自由口通讯基本格式

一个数据帧的组成

对于一个数据帧的组成而言，它是由若干个待发生的字符组成的，从字符1、2到字符n；

一个传输字符的格式：

对于每一个字符的传输格式，它具有1位起始位，7或8位的数据位，0或1位的校验位以及1位停止位；

一个传输字符的485电平：

对于每一个传输字符的485电平，起始位固定为0，数据位和校验位是随机的，停止位固定为1。

自由口同心速波特率可以设置为1200、2400、4800、9600、19200、38400、57600或112500 bit/s。

关于端口协议的选择，字符传输格式，以及波特率的设定需通过设置SMB30（Port0）/SMB130（Port1）来完成。（具体可参照S7-200系统手册）

3）发送指令的使用

自由口的指令一共有两条，一条是发送指令，一条是接收指令。我们在谈及发送或接收的时候往往会对立地去看读或写两个概念，但是读与写，发送与接收并不是相同的概念，一般在谈及读或写的时候往往是基于一些相对gaoji的通讯，比如主从之间的通讯，主站可以对从站进行读或写的操作。相对于读和写的概念而言，发送和接收指令更为基本，例如A和B两个通讯对象，A发送一个报文给B，这是一个发送的过程，B接收到A发送给它的报文，这是接收的过程。而对于读和写则复杂的多，例如A作为主站想要读取B的数据内容，则需要A首先发一个读请求给B，B接收到了A发送过来的读请求之后作出判断，从而将A想要的数据由B再发送给A，由A接收到这个数据从而完成一次读的过程。所以相对读和写，发送和接收的过程要基本的多，而自由口通讯用到的指令就是发送和接收指令。

发送的指令叫做XMT指令（如上图），可以想见它的激活条件必须是一个沿触发，得到沿的时机即为发送指令，向外发送数据的时机。PORT代表的是哪个口向外发数据，CPU224 XP以上的S7-200系列PLC有两个通讯口，PORT=0的时候表示由0口向外发送数据，PORT=1的时候表示由1口向外发送数据。对于TBL而言，这是一个标示着发送数据的地址位，发送的数据格式如下表所示：

4）接收指令的使用

在TBL所指的数据区的第一个数据指的是待发送缓冲区的数据长度，从TBL+1开始则是被发送的数据，被发送数据的长度最多为255个。在上面的程序中，TBL=VB100，VB100当中存的就是待发送数据的数据长

度，以字节为单位，例如如果VB100=5，则被发送的数据是VB101~VB105，VB100本身并不会被发送出去，它仅仅标示被发送数据的长度和位置

在应用自由口通讯时，发送的过程往往比较简单，几乎所有和协议有关的东西都在接收程序里。

接收的指令叫做RCV指令（如上图），该指令同样使用沿触发，PORT同样表示使用0口还是1口，TBL定义的是已经接收了的数据的长度，从TBL+1开始则是已经接收到的数据，n同样是小于255。

例如在上面的程序中，若VB100=5，则已经接收到的数据是VB101~VB105。

在接收过程当中，可以通过SMB86（PORT0）/SMB186(PORT1)来监视接收状态。SMB86/SMB186=0时，表示接收正在进行，否则表示接收已终止。

5）接收过程的定义

接收过程首先执行RCV指令，启动接收，启动之后会进入一种接收等待的状态，等待起始状态的满足，当起始条件满足以后SMB86/186=0，此时数据将按照发送的顺序进入信息缓冲区，直到结束条件的满足，结束条件满足以后SMB86/186不再等于0，之后接收过程结束并产生接收信息完成中断。在整个过程中最为重要的就是起始条件和结束条件，想要将自由口通讯学好，这两个条件是必不可少也是最为关键的部分。

a) 起始条件

上图中将起始条件分为六种：

① 空闲线检测：所谓空闲线检测指的是如果传输线路上的空闲时间大于等于SMW90/190里面所设置的时间的话被认为是一次接收的启动，空闲时间是从RCV被执行的一刻起开始记录，如果在空闲线时间未到的情况下有字符传输进来，那么空闲线时间的计时器将会被重新启动；

② 起始字符检测：对于起始字符的检测是设置在SMB88/188中的一个字符，如果在传输线路中收到了与SMB88/188中设置的起始字符相同的字符，那么被认为是起始条件的满足，从这一刻起传输线路上接收到的数据将会陆续地按顺序进入信息缓冲区，如果检测不到起始字符，则始终处于接收等待的状态；

③ 空闲线和起始字符：它是第一点和第二点的结合，即二者同时满足的前提下才能够被认为是一次起始条件的满足；

④ 断点检测：断点指的是在一个完整的字符传送的时间内，线上的逻辑全部为0。其中一个完整的字符传送时间是指包括起始位、数据位、校验位和结束位在内的一段时间。通常讲起始位固定是0，数据位和校验位也可以都是0，但是结束位一定是1，也就是说在一个完整的字符传送期间之内，线上至少有一刻是为1的，所以断电条件不易满足。这种情况通常应用于通讯对象可以造出一个断点来，那么我们用S7-200PLC可以和它进行断点检测作为通讯起始条件的一种通讯机制。S7-200自身也可做断点，S7-200如果需要发出一个断点，首先在XMT指令使用之前将待发送的数据缓冲区的数据长度定义为0，在这个基础之

上执行一次传送指令，将会有一个断点被发出。如果两台S7-200PLC之间进行断点检测的接收过程，其中一台应该先发一个断点给对方，然后再发数据，这样对方那台以断点检测作为起始条件的PLC将会接到它的数据，双方的通讯就建立了；

⑤ 断点和起始字符：它是断点检测和起始字符检测两个条件相与的关系，同时满足的时候将会作为起始条件的一个设定；

⑥ 任意字符：所谓的任意字符指的是RCV指令一旦执行便无条件地开始起始条件的满足，中间几乎没有接受等待的过程。任意字符也是空闲线检测的一个特例，只是此时SMW90/190是被赋0的，这样就无需任何的等待，一旦RCV指令被执行，起始条件即刻满足，随之而来的数据将直接进入到信息缓冲区。

b) 结束条件

① 结束字符检测：结束字符被定义在SMB89/189中，如果传输的报文中出现了与SMB89/189中相一致的结束字符，接收的过程将结束。结束字符无非就是一个字符，如何能够保证在传输的正常的数据里没有和结束字符相一致的数据呢？使用结束字符检测作为结束条件的应用有一定局限，首先要确保中间的数据不会与结束字符相一致，比如采用ASCII字符传输的过程中， ASCII是有限的一些数，并不是所有的二进制数排列组合都能够在ASCII码表中得以体现，所以此时可以把结束字符定义成为中间传送的数据当中所没有那个ASCII字符来作为结束条件；

② 字符间隔定时器和信息定时器：二者同为定时器且定时时间均由SMW92/192决定，二者之间的区别在于，字符间隔定时器指的是在数据的传送过程中，如果检测到两个字符之间的时间间隔大于SMW92/192里面所设定的时间，那么接收的过程将被终止，而信息定时器指的是从信息开始被接收一旦时间大于了信息定时器所指定的时间，接收将会被终止。

③ 最大字符计数、校验错误、用户结束：三者与前面1、2、3三点不同，前面三点是用户可以自己组态和选择的，而4、5、6后三点是非正常的结束过程。

④ 最大字符计数：是在SMB94/194中指定的最大长度，长度最大可以达到255，如果在接收过程中已经接收到信息缓冲区里面的数据的字节数大于SMB94/194中所指定的数据长度，本次接收过程将会被勒令停止。最大字符计数在使用时一定要记得给SMB94/194赋值，如果未赋值将默认为0，此时即便选择前面三个条件，可是没等前面三个条件满足时，最大字符计数已经勒令此次接收行为终止。

⑤ 校验错误：指的是奇偶校验错误，这种是非正常的结束状态。一旦数据的奇偶校验产生错误，那么当前的这组数据显然是不可以被采信的，此时，数据将会被放弃，接收结束。

⑥ 用户结束：当由于某种原因，用户想提前结束现在正在进行的这次接收行为，那么可以在控制字里面禁止一个位然后执行RCV指令，这样用户条件就结束了，禁止的位其实是SMB87/187的最高位，也就是接收使能位。

注意：

① SMB87/187是自由口通讯控制字，起始和结束条件是通过它来定义的；

② SMB94/194是最大传输字符限制，必须定义。