钦州西门子PLC代理商

产品名称	钦州西门子PLC代理商
公司名称	浔之漫智控技术（上海）有限公司
价格	.00/个
规格参数	品牌:西门子 型号:模块 产地:德国
公司地址	上海市松江区广富林路4855弄88号3楼
联系电话	158****1992 158****1992

产品详情

钦州西门子PLC代理商

基于串行链路的Modbus通信网络是一种主从式网络，在串行网络中只允许存在一个主节点和多247个从节点，在这种网络下，标准ModbusADU中的附加地址域只包含从节点的地址，可寻址范围是0~247，地址0作为广播模式地址使用，从节点地址的有效取值范围是1~247，并且每个从节点的地址必须是的，主节点不存在具体的地址值。主节点设备将要访问的从节点设备的地址放入到请求帧的地址域中，当该地址的从节点设备作出响应时，将会把从节点设备的地址复制到响应帧的地址域中，主节点设备通过该地址得知是由哪个从节点设备发来的响应。

校验域存放了根据报文内容经由冗余校验算法计算所得到的结果。在基于串行链路的Modbus通信网络中有两种传输方式:RTU和ASCII，这两种传输方式的冗余校验算法是不同的。

采用RTU通信模式要比ASCII模式在同样波特率下能传输更多信息，在RTU模式底下是以二进制编码方式对传输数据进行编码，报文中每一个字节(8位二进制位)包含了两个十六进制字符，同一报文内的字符必须连续传输。RTU模式字节传输格式由1位起始位，8位数据位，1位奇偶检验位和1位停止位依次组成，共占用11位二进制位。当不使用奇偶检验时，奇偶校验位也作停止位使用，此时共有两位停止位。RTU传输模式下帧的差错校验域内存放的是报文经过循环冗余检验(CRC)算法计算得出的结果。

采用ASCII通信模式时，每一个字节(8位二进制位)用两个ASCII字符表示。由于每个字节都要用两个字符表示，数据域的长度是RTU模式的两倍，显然在该模式下的传输效率要比RTU模式低。该模式的字节传输格式与RTU模式相似，只是数据位置占用7个二进制位。ASCII模式下帧的差错检验算法为纵向冗余校验(LRC)。

Modbus-TCP实现了在TCP/IP以太网上以客户/服务器方式的Modbus报文通信。这种通信模型是将Modbus

协议作为应用层协议嵌入到低层TCP/IP协议中构成的。与标准Modbus帧相比，Modbus-TCP帧中的寻址与校验交由TCP/IP协议完成。如图3所示，使用封装的方法将ModbusPDU嵌入到TCP报文中形成Modbus-TCP帧，该帧在PDU之前形成了一个占用7个字节大小的MBAP帧头，帧头可以划分为四部分，如表3所示。

交易标识符用于交易校验，服务器端节收到由客户发来的请求交易标识符并复制到响应中。协议标识符用于系统内多路复用传输，取0值时代表Modbus协议传输。长度域记录了该域后续报文的字节长度(包括设备识别符和数据域)，用于服务器识别报文的传输结束。设备标识符用于系统内路由，当需要与通过以太网网关连接的Modbus串行链路或Modbus-Plus通信网络上的设备进行通信时，该标识符域的值由Modbus-TCP客户在请求帧中设置，服务器接收到后，在响应帧中复制该值。

CPU西门子S7-288模块主要包括运算器和高速缓冲存储器及实现它们之间联系的数据、控制及状态的总线(Bus)。它与内部存储器和输入/输出(I/O)设备合称为电子计算机核心部件。

288模块寄存器

包括通用寄存器、寄存器和控制寄存器。

通用寄存器又可分定点数和浮点数两类，它们用来保存指令执行过程中临时存放的寄存器操作数和中间的操作结果。

通用寄存器是CPU西门子S7-288模块的重要组成部分，大多数指令都要访问到通用寄存器。通用寄存器的宽度决定计算机内部的数据通路宽度，其端口数目往往可影响内部操作的并行性。

寄存器是为了执行一些操作所需用的寄存器。

控制寄存器(CR0～CR3)用于控制和确定处理器的操作模式以及当前执行任务的特性。CR0中含有控制处理器操作模式和状态的系统控制标志；CR1保留不用；CR2含有导致页错误的线性；CR3中含有页目录表物理内存基.

通过以太网来实现计算机直接读写PLC数据，使得厂级监控网络能够直接与现场设备通信，监控人员能够在熟悉的计算机画面上对PLC通道进行检测，与依靠人为施加信号来进行检测相比，前者明显地降低了操作人员的工作量，而且当需要检测的IO点数量越大时，效率越高。本程序只是Modbus与TCP/IP协议结合的一个简单应用，虽然以太网的实时性、稳定性和抗干扰性已得到很大的发展，但要把以太网真正应用到实际的控制中还有很多技术难题，这还要走很长一段路。不过以太网进入自动控制领域已是必然趋势，它将使控制变得更加简单和清楚。

Modbus-TCP实现了在TCP/IP以太网上以客户/服务器方式的Modbus报文通信。这种通信模型是将Modbus协议作为应用层协议嵌入到低层TCP/IP协议中构成的。与标准Modbus帧相比，Modbus-TCP帧中的寻址与校验交由TCP/IP协议完成。如图3所示，使用封装的方法将ModbusPDU嵌入到TCP报文中形成Modbus-TCP帧，该帧在PDU之前形成了一个占用7个字节大小的MBAP帧头，帧头可以划分为四部分。

3Modbus-TCP应用

针对施奈德电气旗下的Quantum系列PLC，为了加快完成这方面的工作，采用自编写的程序实现计算机对PLC的四种数据类型直接操作。硬件方面，Quantum系列PLC有能提供以太网接口的网络模块，通过底板与CPU通信，它作为Modbus-TCP通信的服务器，不需要我们做其他编程工作。PLC为上文所陈述的四种数据类型定义了四个独立的内存区，其中离散输入为1区，线圈为0区，输入寄存器为3区，输出寄存器为

4区，寻址方式为区号加上5位的十进制地址，当输入地址不足6位时，系统将自动认为高位数值为内存分区号，其后数值为该区域内的地址编号。由于操作的目的在于检验PLC系统中IO通道的正确性，所需要使用的功能码有:读线圈01、读离散输入02、读保持寄存器03、读输入寄存器04、写多线圈15和写多个寄存器16。

一次完整的Modbus-TCP通信在时间上可以划分为三个步骤:连接的建立、Modbus数据传输和连接的释放。在进行Modbus数据传输之前首先要建立起一个连接，设备是通过在502端口提供一个监听口(socket)来允许与其它设备建立新连接和进行数据传输。当某一设备需要与远方的服务器进行数据交换时，必须通过自身大于1024的端口与服务器的502端口建立连接。TCP连接建立后，客户端设备便可以发送Modbus请求帧到服务器，服务器接收到请求后作出响应，向连客户的端口发送响应报文。传输结束时，客户端负责进行释放通信连接的初始化工作。