

# 齐齐哈尔西门子PLC总代理商

产品名称	齐齐哈尔西门子PLC总代理商
公司名称	浔之漫智控技术-西门子PLC代理商
价格	.00/件
规格参数	
公司地址	上海市松江区石湖荡镇塔汇路755弄29号1幢一层A区213室
联系电话	15221406036

## 产品详情

### 齐齐哈尔西门子PLC总代理商

微机联锁系统中，一般是将联锁置于上位机中，这样安全性、可靠性得不到保障。文中用西门子S7-400HPLC完成联锁功能，构成PROFIBUS-DP/MPI分布式网络系统，这样整个联锁系统安全可靠。通过介绍DP/MPI网的概念和实现，结合唐山钢铁公司焦化站联锁实例，着重阐明用PLC实现DP/MPI网络，以解决该联锁系统中分布式输入输出等。经现场调试、安装，整个网络运行良好，安全可靠地实现和完成车站信号联锁系统的联锁功能，应用前景很好。关键词：现场总线;可编程逻辑控制器;

开放式系统互联引言 车站联锁系统是铁路信号系统中的一个重要组成部分，它的主要任务是控制车站中的信号机和道岔，并且对信号灯状态进行处理和对进路进行选择等。随着铁路信号系统的信息化发展，微机联锁系统必然取代旧式的电气联锁系统。就国内外现状来看，大多采用上、下位机的办法来实现对车站信号的控制;有些微机联锁系统中，下位机主要实现数据的采集、命令发送、数据输出等，而把主要的联锁功能置于上位机，这样一来，上位机负担太重，一旦上位机产生故障，不能保证系统的安全性、可靠性。如果能够将联锁功能块置于下位机，而且下位机安全性、可靠性比较高，那么整个系统的安全性、可靠性就能够得到有效保证。在以前的微机联锁系统中，用工业控制机作为下位机，实现联锁功能，但不能保证系统冗余，这样就不能保证整个系统的安全性、可靠性。因此，就要不断更新和研究，寻求更完善的、更可靠的硬件、软件环境，以提高系统性能和安全系数。用西门子PLC完成联锁功能，构成PROFIBUS-DP/MPI分布式网络系统，这样整个联锁系统安全可靠。PROFIBUS现场总线技术是随全数字信号系统的发展而产生的，是由德国组织开发的工业现场总线协议标准——PROFIBUS现场总线标准（DIN19254）。PROFIBUS是近年来国际上为流行的现场总线，也是目前数据传输率快的一种现场总线（传输率可达12M波特），因此在很多领域内广泛应用。它是不依赖于生产厂家的、开放式的现场总线，各种各样的自动化设备均可通过同样的接口交换信息。PROFIBUS-DP（DistributedI/O-分布系统）是一种经过优化的模块，有比较高的数据传输率，适用于系统和外部设备之间的通信，远程I/O系统尤为适合。它允许高速度周期性的小批量数据通信，适用于对时间要求比较高的自动化场合。笔者将以S7-400HPLC为例，结合其在铁路信号中的应用，探讨实现PROFIBUS-DP/MPI网络系统原理和方法。PROFIBUS-DP/MPI网的性质和特点 PROFIBUS-DP适用于现场层的高速数据传送。主站周期地读取从站的输入信息并周期地向从站发送输出信息。除周期性用户数据传输外，PROFIBUS-DP还提供智能化现场设备所需的非周期性通信以进行组态、诊断和报警处理等。DP网的协议结构 PROFIBUS定义了各种数据设备连接的串行现场总线的技术和功能特性，这些数据设备可以从底层（如传感器

、执行器层)到中间层(如车间层)广泛分布。PROFIBUS连接的系统由主站和从站组成。主站一般要复杂些;从站为简单的外围设备,典型的从站为传感器、执行器及变送器,它们没有总线控制权,仅对接收到的信息给予回答,或者主站发出请求时回送给主站相应信息。因此,从站只需要协议的一小部分,实现起来非常方便。PROFIBUS协议结构是根据ISO7498,以开放式系统互连网络(Open System Interconnection, OSI)作为参考模型,该模型共有7层,PROFIBUS-DP定义了其中的、二层和用户接口。第3到7层未加描述。图1为ISO/OSI参考模型与PROFIBUS体系结构比较。用户接口规定了用户及系统以及不同设备可调用的应用功能,并详细说明了各种不同PROFIBUS-DP设备的设备行为。物理层采用EIA RS-485双绞线或光纤,连接器采用RS-485标准的9针D型插座。数据链路层提供了介质存取控制功能、数据的完整性检查以及传输执行的协议,在PROFIBUS中称第2层为现场总线数据链路(FDL)(包括介质访问存取控制(MAC)子层、现场总线链路控制(FLC)子层、现场总线管理(FMA1/2)子层),采用混合介质存取协议,对应于DIN(E)19245,支持单主或多主系统,主或从设备,大站数为126。它包括主站之间的数据传输的令牌环方式和从站之间的主-从方式。PROFIBUS第7层包括底层接口(LLI)、现场总线信息规范(FMS)和现场总线管理(FMA7)。图1 ISO/OSI参考模型与PROFIBUS体系结构比较 图2为PROFIBUS-DP数据传输示意图,即主站发送请求,访问DP从站,其中包括帧格式;从站收到请求信息后,立即响应主站,并回送响应帧。图2 PROFIBUS-DP用户数据传输DP网的性质及特点 PROFIBUS—DP采用主从方式和低层的令牌环传递相结合的形式进行通道分配,整个网络可以将总线系统分割成线段,分步建立,段间用中继器连接,每个段可以有32个网络站,整个网络可以达到126个网络站。由于大传输速率可达12Mbps,以及其第2层采用SRD(发送并要求回送)功能,使得输入、输出数据可以在一个周期内完成,所以传输速度提高了,可尽可能地减少总线周期。而在单主站系统中只有一个主站,这种组态提供了短的总线周期。PROFIBUS-DP开放性好,开展性强,灵活性高。用S7-400H PLC构成DP网,由于SIMATIC S7 V5.2提供有效的系统支持,可实现软件参数化I/O、多功能自诊断,功能模块更易于连接。在S7-400H系统中,CPU之间的同步,由同步模块通过同步光纤连接,在软件和硬件方面都可以实现CPU同步。采用STEP 7编程软件进行现场集中控制编程,诊断测试就象采用集中处理单元的集中编程接口时一样。在编程过程中,不需考虑硬件配置,由编程软件实现网络系统组态。MPI网的性质和特点 CPU中用于连接象编程器这样的设备的接口叫多点接口(MPI),这是因为通过这个接口,两个或两个以上的设备可以从两个或两个以上的节点与CPU通讯。也就是说,带有MPI的CPU已经具有连网能力。MPI网络的结构与PROFIBUS-DP网络是相同的,就是说,两种网络遵循的规则和使用部件是相同的。S7-400H PLC实现的DP/MPI网络系统 下面是一个按照上述原理用S7-400H PLC构成的多主站DP/MPI网络的实例。系统结构 整个网络系统为一个车站信号的控制,如图3所示。该网络为由两台S7-414H PLC和ET200M组成的分布式结构。PLC通过CP 5611卡与上位机通信。其中一台PLC为主站,另一台为热备。ET200M选用西门子IM153-2。IM153-2的作用是连接I/O模板,提供PROFIBUS-DP连接;输入模块选用SM321 DI32 × DC24V,共需要18个模块,主模块9个,备用9个。输出模块用SM322 DO32 × 24V,共用8个,主模块4个,备用4个。输入、输出模块都是通过 DP连接。3台上位机,都是通过CP5611与PLC的CPU相连。两个CPU之间通过同步光纤连接。用户界面 每台PLC都通过CPU模块上的MPI集中编程接口和配置有MPI接口的PC机相连。我们采用西门子的CP5611与PLC的CPU相连。PC机中配置SIMATIC STEP 7 V5.2编程软件。由于是冗余系统,还需要安装西门子的冗余软件,才能做到PLC的两个CPU之间同步。3台上位机中,其中两台是操作员用的监控机,另一台为维修机。在整个系统中,上位机之间可以互相通讯,也可以与PLC之间通讯。每台PC机都要安装CP5611驱动软件,才能完成功能。程序结构 系统组态及参数设置 由SIMATIC STEP 7 V5.2编程软件,进入硬件组态状态,对各台PLC进行网络参数设置。首先,建立Project,如取名为C:\swjtu,在该文件下选择网络 Subnet为PROFIBUS,站名为SIMATIC414HStation,然后进行硬件组态。其次是建立各站在网络的地址。后组态3个PG/PC站,在选项窗口中选中CP5611,并分配地址,主编程站地址为0,其余两个只要地址不相同即可。程序结构 西门子SIMATIC S7-400H PLC的编程器STEP 7可运行在PC机的bbbbbbbs环境下,界面友好,提供了梯形图、语句表和块图3种形式的编程、调试、诊断等功能。本实例采用模块化程序结构,程序由几大功能块组成,每个功能块完成一系列的控制逻辑,放置在组织块OB1中的指令决定控制程序的各功能块的执行。本例zhonggong能块FC1是微机联锁命令处理程序,FC2是进路处理程序,FC3, FC4是微机联锁状态处理程序,FC5是常量定义,FC6是信号输出处理,FC7是道岔输出处理,FC8是信号采集。程序结构框图如图4所示。功能块为多层次调用,FC1在调用其他功能块,比如FC1调用FC9, FC9调用FC10, FC10调用FC11、FC12、FC13、FC14等。在STEP 7中,允许功能块调用多为16层。图3为应用于唐山钢铁集团公司焦化厂火车站的微机联锁系统的PROFIBUS-

DP/MPI网络原理框图。3台监控机为监控层，PLC为联锁层，I/O为控制层。车站联锁系统主要由联锁以及信号、道岔、区段和进路的动作建立。本例中，以车站微机联锁的控制过程说明PROFIBUS-DP网络的实践应用。图3网络系统结构图进路控制过程包括进路建立、进路解锁。进路建立包括进路选择、道岔控制、进路锁闭、信号控制，进路解锁就是对已建立的进路、道岔进行的进路锁闭，进路解锁包括取消进路、人工解锁、正常解锁、中途折返解锁、故障解锁。图4程序结构框图在组织块OB1中，先调用FC1对联锁命令进行处理，其中包括进路处理、道岔处理、信号处理，调用FC2对进路进行处理，调用功能块FC1、FC2对联锁状态进行处理，再调用功能块FC6、FC7、FC8对数据进行输入输出处理。以功能块FC1命令处理程序为例，说明其功能调用过程。功能块FC1先调用FC10进行进路选择，然后调用FC11、FC12、FC13等，对其他命令进行处理。结论从实际应用来看，整个网络运行良好，网络结构简单，技术性能稳定。实践证明，PROFIBUS-DP网构成的灵活实用分布式网络在铁路系统有良好的应用前景。

德国西门子（SIEMENS）公司生产的可编程序控制器在我国的应用也相当广泛，在冶金、化工、印刷生产线等领域都有应用。西门子S7系列PLC体积小、速度快、标准化，具有网络通信能力，功能更强，可靠性更高。S7系列PLC产品可分为微型PLC（如S7-200），小规模性能要求的PLC（如S7-300）和中、高性能要求的PLC（如S7-400）等。

**SIMATIC S7-200 PLC S7-200**  
PLC是超小型化的PLC，它适用于各行各业，各种场合中的自动检测、监测及控制等。S7-200 PLC的强大功能使其无论单机运行，或连成网络都能实现复杂的控制功能。S7-200 PLC可提供4个不同的基本型号与8种CPU可供选择使用。

**SIMATIC S7-300 PLC S7-300**是模块化小型PLC系统，能满足中等性能要求的应用。各种单独的模块之间可进行广泛组合构成不同要求的系统。与S7-200 PLC比较，S7-300 PLC采用模块化结构，具备高速（ $0.6 \sim 0.1 \mu s$ ）的指令运算速度；用浮点数运算比较有效地实现了更为复杂的算术运算；一个带标准用户接口的软件工具方便用户给所有模块进行参数赋值；方便的人机界面服务已经集成在S7-300操作系统内，人机对话的编程要求大大减少。SIMATIC人机界面（HMI）从S7-300中取得数据，S7-300按用户指定的刷新速度传送这些数据。S7-300操作系统自动地处理数据的传送；CPU的智能化的诊断系统连续监控系统的功能是否正常、记录错误和特殊系统事件（例如：超时，模块更换，等等）；多级口令保护可以使用户高度、有效地保护其技术机密，防止未经允许的复制和修改；S7-300 PLC设有操作方式选择开关，操作方式选择开关像钥匙一样可以拔出，当钥匙拔出时，就不能改变操作方式，这样就可防止非法删除或改写用户程序。具备强大的通信功能，S7-300 PLC可通过编程软件Step 7的用户界面提供通信组态功能，这使得组态非常容易、简单。S7-300 PLC具有多种不同的通信接口，并通过多种通信处理器来连接AS-I总线接口和工业以太网总线系统；串行通信处理器用来连接点到点的通信系统；多点接口（MPI）集成在CPU中，用于同时连接编程器、PC机、人机界面系统及其他SIMATIC S7/M7/C7等自动化控制系统。

**SIMATIC S7-400 PLC S7-400**  
PLC是用于中、性能范围的可编程序控制器。S7-400 PLC采用模块化无风扇的设计，可靠耐用，同时可以选用多种级别（功能逐步升级）的CPU，并配有多种通用功能的模板，这使用户能根据需要组合成不同的专用系统。当控制系统规模扩大或升级时，只要适当地增加一些模板，便能使系统升级和充分满足需要。

随着中国工业经济的发展，PLC在中小型自动化设备的日益普及应用，对于设备制造厂商或生产技术管理部门来说，如何以快捷的方式响应现场设备维护方面的需求，迅速检测生产现场运行设备的状态，及时解决生产现场反映的问题，已是多数上位技术管理者的切实需求。如何采用经济实用的方式来实施远程PLC设备数据采集或测控，这也是探索解决此问题的初衷。

## 1、系统组成概述

系统硬件主要由上位计算机、TC35i GSM MODEM无线通讯模块和远程Siemens S7—200 PLC 3部分组成，具体结构如图1所示。系统软件分为上位PC和下位PLC两部分，上位PC部分提供人机交互操作界面和相应的数据选择、处理等；下位PLC则通过自由口通讯，以中断方式快速响应上位机对PLC变量存储器数据的读写操作或对I/O口读写操作需求。由于上位计算机与远程PLC的通讯载体是通过TC35i建立在GSM网络基础上的，从而打破了地域的限制，即便远端PLC设备在千里之遥，实施数据采集、测控的如同咫尺

## 2 系统硬件设计

### 2.1 TC35i无线通讯模块

系统组成如图1所示，系统硬件主要是TC35i无线通讯模块的应用。TC35i是Siemens公司推出的新一代无线通信GSM模块，TC35i双频工作(EGSM900 / GSM1800)，电源范围在3.3 ~ 4.8 V，发送功率分别为2W(Class4 EGSM900)和1W(Class1 GSM1800 MHz)，TC35i的数据接口采用串行异步收发，符合ITU-TR3232接口电路标准。数据接口配置为8位数据位、1位停止位、无校验位，可以在300 ~ 115 kb / s的波特率下运行，支持的自动波特率为4.8 ~ 115 kb / s，符合ETSI标准GSM0707和GSM0705，且易于升级为GPRS模块。该模块集射频电路和基带于一体，向用户提供标准的AT命令接口。为数据、语音和短消息提供快速、可靠、安全的传输，方便用户的应用开发及设计。TC35i有40个引脚，通过ZIF连接器引出。这些引脚可划分为5类，即电源、数据输入 / 输出、SIM卡、音频接口和控制。TC35i内部电路如图2所示。

ZIF40PIN的引脚1 ~ 14为电源部分，其中引脚1 ~ 5为电源电压输入端VBATT+，引脚6 ~ 10为电源地GND，引脚11 ~ 12为充电端，引脚13为对外输出电压(供外部电路使用)，引脚14 ACCU / TEMP接负温度系数的热敏电阻；引脚24 ~ 29为SIM卡连接端；引脚33 ~ 40为语音接口用来接电话手柄。引脚15、30、31和32为控制部分，引脚15为启动线IGT(Ig-niI Ion)。当TC35i通电后必须给IGT一个大于100 mV的低电平，模块才能启动。引脚30为RTC back up；引脚31为掉电控制；引脚32为SYNC，引脚16 ~ 23为数据输入 / 输出端。TC35i无线通讯模块的主要外围电路的连接如图3所示。数据通信电路以MAX232为核心实现电平转换及串口通信。

### 2.2 系统硬件连接

系统硬件的连接可参考图1可知，上位计算机的串口输出与由TC35i构成的GSM MODEM中的9芯RS232口直接连接；远程的GSM MODEM与PLC连接时则必须通过RS232到RS485的转换，这是Siemens PLC的通讯口数据和PPI编程电缆连接的必要条件。另一方面必须注意的是，在与远程GSM MODEM的RS-232串口连接时，还必须将RS232串口中的RXD和TXD对换连接，否则将不能正常通讯。

### 2.3 远程PLC的选型

该系统选用西门子S7—200 PLC，在西门子PLC中SIMATIC S7—200是一个系列，其中包括多种型号的CPU，这里选用CPU-222，由于CPU不提供模拟量的输入输出，为检测对模拟量数据的远程读写。因此在远程PLC系统中扩展一型号为EM-235的4输入1输出模拟量模块。

## 3 系统软件设计

### 3.1 系统上位计算机人机界面

系统上位的人机界面是用VB编程，提供人机交互操作界面及数据选择和相应的数据处理等功能。系统上位的操作界面如图4所示。在操作界面的左上部是通讯链接控制框，这里只需要正确选择PC的串口并输入远程PLC所连接的电话号码后即可拨号链接，远程的无线GSM MODEM模块摘机响应一般设置为铃响后自动摘机，通讯链接建立后，当上位PC检测到串口端的数据载波DCD信号后，通讯链接控制框中的“链接状态”指示灯由红变绿，表示通讯链路已成功建立。拨号或挂机的操作均是通过对GSM MODEM模块发送AT指令执行的。

对PLC数据的读写操作如操作界面的右上部所示，在相应文本框内填写好数据的类型、地址、数值和操作方式后点击“发送”即可执行对PLC的读或写操作。界面的下半部分显示的是PC串口发送和接收的代码以及当前操作的结果。

### 3.2 系统上位计算机的串口设置

在上位PC的人机界面中，串口的设置是通过下拉选择框选择出所连接的串口后由程序自动读取。在使用GSM MODEM无线模块时，上位PC对远程PLC链接呼叫时采用的是AT指令。程序语句为：MSComm1.Output=“ATDT”&Trim(Text1.Text)&vbCrLf//Text1文本框内为欲连接的电话号码。挂机的AT指令为：MSComm1.Output=“ATDT”&“+++”&vbCrLf。串口数据格式的设定语句为：MSComm1.SetTIngs=“9600.N,8.1”，与TC35iGSM MODEM无线通讯模块和远程PLC自由口的串行数据通讯格式一致。

### 3.3 通讯数据格式的约定

由于远程PLC采用的是自由口用户通讯方式，这里对每次收发数据字节暂约定为18个字节，数据字节的多少可根据实际需要而酌情约定。本系统中18个字节的约定：Bybbb为数据的总字节数；Bvte2为数据开始特征字；Bvte3为数据读或写特征字；Byte4为数据类型特征字；Bvte5~Byte8为PLC数据地址；Bvte9~Bybbb6为PLC数据的数值；Bybbb7为收发数据的校验码；Bvbbb8为数据结束特征字。串口数据的传输除数据地址字节和数据数值字节用ASCII码表示外，其他均以十六进制方式表示。因而在上位PC的编程中需涉及大量的进制转换操作。特别要注意的是由于PLC中的实数采用32位单精度数表示，并按照ANSI/IEE E745 1985标准格式以双字长度来存取，所以无论是上位的PC或是下位的PLC在编程时对实数数据的处理均需严格遵循ANSI/IEE E745 1985标准格式的规定，否则将不可能读到正确的数据。

通讯数据的校验方式采用BCC块进行XOR校验，即约定为从每次数据包的Byte2到Bybbb6的字节进行校验，Bvbbb7存放校验结果。上位或下位在接收数据时，首先对所接收的数据进行校验并将计算结果与Bvbbb7所存放的数值进行比较，如不一致时则按约定要求重发，以保障每次传输数据的正确性。

### 3.4 远程PLC自由口通讯初始化编程

由于远程PLC采用的是自由口用户通讯协议，所以对PLC的自由口通讯必须做如下初始化设置：

远程PLC经上述设置后，在其运行期间每当接收到一组数据后便自动产生中断请求，在中断服务的子程序中，设定一标志位(如M0.0)置位，用来表示允许进入中断服务，在主程序中通过检测M0.0的状态来确定是否转入读数据操作的子程序，读数据操作完毕后及时将接收数据标志M0.0复位，从而完成一次读数据过程。PLC数据的上传则是根据所读数据的内容来响应上位的请求，上传数据的编码和字节均依照约定的格式写入，每次的读写操作仅在PLC一个扫描周期内(数毫秒)完成，系统的响应是实时的。

### 3.5 远程PLC数据的读写操作

PLC数据的读写是依据约定的数据类型实施操作的。对于字节、字、双字、实数及I/O端口各自有约定的数据类型特征字，在下位PLC程序中通过对数据类型特征字的解析后来确定读取数据的字节数。对I/O端口的读写操作则是根据约定的地址编码直接读写出相应的状态信息。每组收发数据的存储单元从VBI00到VBI17共18个字节。由前述的数据发送量的约定可知，每组数据的Byte5~Byte8表示PLC数据的地址，由于每次读写的地址是不同的，所以Byte5~Byte8字节给定的就是地址指针，在PLC编程中就要以此指针采用间接寻址的方式，假设Byte5~Byte8存放在PLC的VB104~VBI07单元，其间址指令则为：

MOVD &VBI04, ACI读取该地址内容时则根据数据类型的不同而有所区别，假如读写字节时指令为：MOV B \*ACI, VBI60；则读写字的指令为：MOVW \*ACI, VWI60；读写双字的指令为：MOV D \*ACI, VDVI60

\*ACI, VDI60; 读写实数的指令则为: MOV R \*ACI, VDI60。

#### 4 结束语

本系统经实际测试基本达到了预期效果。远程PLC在省际间距离的测控响应与在本市区地域的测控响应基本相同,通过对PLC I/O的读写、模拟量数据的读写、单字节、双字节及实数的读写,均未出现数据差错现象,远程的响应速度基本上是对上位的指令立即响应,操作人基本感觉不出时间的延时。在PLC中,由于本远程测控程序字节量较少,完全可以嵌入在PLC的过程控制程序中运行,由于在自由口通讯中

对上位PC读写的响应采用的是中断方式快速响应,所以对PLC的过程控制程序的实时性基本无影响