廊坊西门子PLC总代理商

产品名称	廊坊西门子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

廊坊西门子PLC总代理商

现场总线的特点是开放、互联，这是它优于其它形式系统的根本原因。但是这种开放互联的性质也给现场总线系统带来了不安全因素。讨论了现场总线系统的通信安全问题，指出这一问题的重要性，提出了在设备层实现通信安全的方案。根据现场总线技术的特点和发展现状提出了模块化的加密方案，并且对这一方案的适用性进行了分析，同时也探讨了其对总线通信性能的影响。 我国已经提出了“ 以信息化推动工业化 ”的战略。在生产自动化系统中实现信息交换和共享并以此为基础实施企业CIMS工程已成为人们的共识，这必将成为自动化系统未来发展的方向。现场总线在这一系统中扮演了重要的角色，它为底层的智能设备提供了开放的通信平台，使之能够实时地进行数据交换。而且便于自动化系统与企业局域网互联，从而实现任意时刻、任意地点的控制，进而推进整个企业的自动化、信息化进程。
一、问题的提出 图1为某中药生产厂的自动化系统。该系统实现了中约生产中的配料工作的自动化，能够提高生产效率，而且增加保密性，同时便于远程管理。
图1 中药配料系统 在生产一线上采用基于现场总线的控制系统。当中药配料落入秤斗中时，Panther仪表就可以检测出这个变化，经过A/D转换变成以数字表示的称重数值。通过RIO接口，PLC程序可直接读取Panther的称重数值。智能仪表与控制器作为总线节点，依托总线进行相互通信，协调工作。 可以看到基于现场总线的这一系统结构简单，成本较低，可以有灵活的控制，可扩展性强。而且能够方便地与企业局域网进行通信，从而满足远程控制的要求。 可是我们发现，在现场总线一级的设备之间的通信是不安全的，如图2中，监听者可以获取信道中的数据。现场总线协议标准是公开的，这些数据很容易被解释为有意义的信息，那么各个节点之间的通信就没有任何保密性可言。 现场总线数据交换中的这种不安全因素来自于协议本身。现场总线采用类似局域网的广播报文方式进行通信，那么上面的这种窃听就可以获取总线上通信的所有信息。对于一个中药厂来说，药品的配方就是企业的生命，如果这些信息被窃取，后果将不堪设想。 推而广泛，现代企业的许多关键技术都会在生产一线的仪器工作参数中体现出来，那么随着企业的自动化、信息化程度的提高，信息的不安全性也越来越高。企业的现代化进程是不可避免的，在这一过程中，必须对信息安全提出越来越高的要求，对于采用现场部构建的生产自动化系统，应该考虑总线网段的通信安全。 二、解决方案
我们提出的是一种进行设备间通信加密的方案，来解决上面提出的问题。 现场总线网段上设备的通信加密不同于目前通常的网络通信加密，，需要考虑实现加密的层次、实现方法以及对性能影响等诸多因素。 1、实现安全的层次

1 引言可编程控制器是以微处理器技术为基础，综合了计算机技术、自动化技术和通讯技术的一种新型工业控制装置。其可靠性极高、耐恶劣环境能力强、使用极为方便等特点，与机器人技术、CAD/CAM并列称为工业生产自动化的三大支柱。它是上世纪60年代发展起来的被国外称为“先进国家三大支柱”之首的工业自动化理想控制装置，是近年来发展极为迅速，运用面极广的工业控制装置，现已广泛运用于自动化的各个领域。

2 可编程序逻辑控制器(PLC)PLC 英文名Programming Logic Controller 即可编程序逻辑控制器，是早于汽车制造行业应用并发展起来的一项技术，用于代替继电器完成机器和设备的自动控制，它的大的特点是可编程，即根据控制逻辑和控制要求的变化可重新编制程序，而不用象继电器线路一样需要重新更换原器件和重新接线。PLC已集成了许多计算功能、通信功能、完成特殊控制功能的功能模块如位置控制、速度控制、过程控制等，并具有了与计算机系统的集成和连网的能力，PLC自发明以来在工业自动化、交通控制、电力运输、楼宇自动化等领域得到了广泛的应用。

3 PLC发展历史自1969年世界上台可编程控制器在美国DEC公司诞生以来，PLC走过了30余年的发展历程。回顾其发展历程，可将PLC技术分为3个阶段:(1)
传统PLC阶段。它是PLC的初阶段，也是现代PLC的基础。其结构如图1所示，工作原理 如图2所示。如图2所表示的一样，PLC的工作原理是:首先读取输入接点的状态→然后执行程序→然后根据程序的执行结果刷新输出接点的状态→然后再读取输入接点的状态→读取输入接点的状态,如此循环执行。

由PLC的工作原理可以看出:从输入端的信号状态发生变化到输出端的信号变化，中间需要执行程序(用户程序、系统程序)，程序的执行需要时间，而且这个时间是不可预测的，在某些应用场合这是不允许的，如位置控制、速度控制、需要高速响应的控制，这就使得PLC在这些场合不能使用或需配置昂贵的专用模块。从图1可知，PLC系统的核心是微处理器(CPU)，为防止系统程序跑飞，产生误动作，必须采取一系列硬件和软件的措施去克服这一问题，同时由于PLC使用的是梯形图语言，系统本身必须带有功能强大的编译器，这样就使得PLC构成的系统具有较高的价格。而且程序跑飞、编制的程序出现死循环等依然是存在的隐患问题。(2) OPEN PLC阶段。OPEN PLC又称PC BASE PLC、SOFT
PLC，是近几年提出的一种概念，它是基于开放式PC
平台和开放式开发软件的PLC，它能方便的与其他软件集成及网络集成。其组成结构如图3所示。

OPEN PLC只是在它的开发环境方面提出了一个新的概念，即开放性、标准化，它的运行原理方面与传统PLC相比具有实时多任务运行机制，但仍然是基于程序执行这样的基础。因此它并没有从根本上解决传统PLC存在的问题，在其实现的系统中依然存在。

(3) 现场集成阶段。也就是HARD PLC阶段，它是一个全新的代名词，也是一个PLC的新发展动向。它采用现代可编程逻辑器件CPLD/FPGA(Complex Programmable Logic Devices & Field Programming Gate Array)作为硬件平台，采用EDA(Electronics Design Automation)开发工具配与硬件描述语言HDL(Hardware Debbbbbbion
Language)做为开发软件平台，象传统PLC一样它同样是可编程的。其组成结构图如图4所示。

HARD PLC则抛弃了传统PLC“程序”的概念，以“硬件线路”来实现控制功能，而编程改变的也只是其芯片内部的硬件连接，而不需运行软件程序，因此自然没有程序跑飞、开机复位及自带语言编译器等问题，其完成的功能与传统PLC相同，而系统的造价仅是传统PLC系统的十分之一，甚至更少。在硬件线路运行时所有的信号是并行运行的，而且信号的路径是可知的，信号传输的时间是可预测的，所以可用于jingque控制的需要，如位置控制、速度控制、信号处理、图像处理、高速机械等。它从根本上解决了传统

PLC存在的不足，代表了传统PLC的终发展方向。

4 PLC的发展趋势随着微处理器技术、超大规模集成电路技术和数字通讯技术的进步和发展，可编程序控制器也得到了迅速发展，其功能已远远超出了其定义所指的范围，其概念也日趋模糊，现代可编程控制器的发展趋势主要有以下几个方面:(1)
用高性能器件，尽量缩小与工业控制计算机之间的差距。例如，德国FESTO公司的IPC(Industrial PC)由一系列符合工业标准的模块组成，它与微机兼容且具有PLC的功能。(2)
丰富I/O模块，使PLC在实时性、精度、分辨率、人机对话等性能方面进一步得到改善和提高。(3) 进一步强化网络功能，以实现信息管理自动化。例如IPC型控制器具备多种现场总线接口。如FESTO总线、Profibus、AS-I、CAN等，以及各种网络连接模块，如Novell等，从而使PLC与PLC、PLC与PC、PLC与现场设备之间建立通讯联网。(4) 多种编程语言并存，互补不足。IPC型控制器除了采用梯形图、指令表编程以外，还可以用IEC1131规定的用于顺序控制的标准化语言以及C、Basic等计算机语言进行编程。(5)
硬件结构集成化、冗余化。随着专用集成电路(ASIC，Application Specific Integrated Circuits)和表面安装技术(SMT，Surface-Mout Technology)在PLC硬件设计上的运用，使得PLC产品硬件元件数量更少，集成度更高，体积更小，其可靠性更高。同时，为了进一步提高系统的可靠性，PLC产品还采用了硬件冗余和容错技术。用户可以选择CPU单元、通信单元、电源单元或I/O单元甚至整个系统的冗余配置，使得整个PLC系统的可靠性得以进一步加强。

5 可编程控制器现场集成技术研究的意义现行的可编程控制器均是由专门的生产厂商设计生产的，用户选用他们提供的专用控制器时，可能只用到它的部分功能，会造成一定的资源浪费，而且专用控制器价格高，不经济。而使用现代可编程逻辑器件来实现具有如下优点:(1) 用户可以根据需要设计控制器的功能，不会造成太大的资源浪费;而且不用带自身专用的编译器，从而大大降低了系统的价格。(2) 用户逻辑和接口部分可以做在同一个器件内，因而让接口和用户逻辑更紧密地结合;用FPGA/CPLD芯片组成的系统，很自然地避开CPU的程序跑飞、死循环、复位不可靠等缺点，无需采用过多措施就能使系统具有很高的可靠性。(3) FPGA作为控制器的核心，其灵活的现场可更改性、可再配置能力，对系统的各种改进非常方便，在不更改硬件电路的基础上可以进一步提高系统的性能，也就是完成硬件的在系统升级;在线编程是FPGA/CPLD突出的特点，它无需改变芯片外部I/O口的连接线，可直接在用户自己设计的目标系统中或线路板上对FPGA/CPLD器件编程，这就打破了使用一般数字器件和PLC先设计后装配的惯例，而可以先装配后编程，用在实际系统后还可以反复编程，从而开创了数字电子系统设计技术的新一页。此外，还可以通过红外线编程、超声波编程或通过电话线、Internet进行在线编程。这些功能在远控或军事领域上有特殊的用途。(4) FPGA的性能价格比很高，用它实现的控制器的价格，几乎只是和它具有相同输入/输出端子市售可编程控制器价格的十分之一;而且其逻辑实现是并行工作的，其速度远远大于PLC，这在实时系统中是非常有优势的。(5) 它抛弃了传统PLC“ 程序 ”的概念，以“ 硬件线路 ”来实现控制功能，在硬件线路运行时所有的信号是并行运行的，而且信号的路径是可知的，信号传输的时间是可预测的，所以可用于jingque控制的需要，如位置控制、速度控制、信号处理、图象处理、高速机械等。从以上优点我们可以看出，基于FPGA/CPLD的HARD PLC能更经济、更稳定、更方便地适应用户的需求，而且其实时性、灵活性远远优于传统的可编程控制器(PLC)。因此，可编程控制器的现场集成技术应用非常广阔，具有很强的工程实用价值。

1 引言在一个自动监控(Supervisory Control And Data Acquisition SCADA)系统中，投入运行的监控组态软件是系统的数据采集和处理中心、远程监控中心和数据转发中心。处于运行状态的监控组态软件与各种控制、检测设备如挂接在现场总线上的工控计算机、PLC、智能仪表、智能设备等共同构成快速响应控制中心。控制方案和算法一般在设备上组态并执行，也可在工控计算机上组态，然后在下装到设备中执行，根据设备的具体要求而定[1]。组态软件在SCADA系统中所处的位置如图1所示。监控组态软件投入运行后，操作人员可以在其支持下完成以下各项任务:(1)
查看生产现场的实时数据及流程画面，浏览各实时/历史趋势画面;(2)
自动打印各种实时/历史生产报表;(3) 及时得到各种过程报警和系统报警;(4)
在需要时，人为干预生产过程，修改生产过程参数和状态;(5)
与管理部门的计算机联网，为管理部门提供生产实时数据。

图1 监控组态软件在SCADA系统中所处的位置

现场总线作为开放的控制网络能实现现场设备间、现场设备与控制室间的信号通信[2]。开放通信是信息传输与共享的基础之一，而当现场信号传至监控计算机之后，如何实现计算机内部各程序之间的信息沟通与传递，即如何让现场信号与各应用程序连接起来，让现场信息出现在计算机的各应用平台上，依然存在一个连接标准与规范的问题。在多用户、多任务的计算机系统中实现程序间的数据交换比较方便，操作系统对这种操作是支持的。自从bbbbbbs及微机版UNIX、LINUX操作系统的面世后，出现了程序之间交换数据的技术、协议或标准，实现程序间的数据交换才比较容易。在工业PC机的自动化系统中被广泛采用的，让现场总线控制系统和人机界面软件能够有效充分地用PC机丰富强大的软件资源，是一项值得深入研究的课题。文章对有关技术问题结合工程实践作些讨论。2 动态数据交换的基本概念尽管工控组态软件的数据交换技术有了长足进步，在当前实际运用的现场总线控制系统组态软件中，对于DDE和OPC两种数据交换技术的具体运用—特别是在微机执行多任务条件下如何进一步提高组态软件与其他程序之间的数据交换实时性方面，仍然存在某些不足，值得进一步探讨和研究。其中，动态数据实时交换(DDE)技术在控制网络的集成中得到了实际应用。其原因:(1)
这种方法实时性较好，可以采用标准的bbbbbbs技术;(2) 作为连接控制网络与信息网络的通信处理机在硬件上比较容易实现。当控制网络与信息网络有一共享工作站或通信处理机时，就可以通过动态数据交换技术实现控制网络中实时数据与信息网络中数据库数据的动态交换，从而实现控制网络与信息网络的集成。DDE是进程间通信的方法。为了进行会话，DDE应用程序用3个基本的标志符(或字符串)，即三层识别系统来区别其他DDE应用程序，他们分别是应用程序名(Application)、主题名(Topic)和项目名(Item)。每个DDE会话由应用程序名和主题名唯一定义，在DDE会话建立前由客户程序和服务器共同决定应用程序名和主题名，而由客户程序填写服务器的3个标志名。应用程序名位于层次机构的顶层，用于指出特定的DDE服务器应用程序名。主题名更深刻地定义了服务器应用程序会话的主题内容，服务器应用程序可支持一个或多个主题名[2]。3 面向过程控制的动态参数数据交换程序设计为方便讨论问题、现举例说明。根据某生产自动化改造工程要求,需要对系统进行组态监控操作平台设计，采用组态软件IFIX2.2和bbbbbbs应用软件VB6.0，开发并实现基于DDE机制的进程间数据交换，满足工业控制网SCADA工控计算机内部信息交换需要，为各应用程序通过共享内存交换信息，实现控制网络与信息网络的集成，并为进一步进行bbbbbbs程序间的数据交换开发提供有借鉴意义的参考[3]。控制网络与信息网络的主要集成技术如图2所示。

图2 控制网络与信息网络的主要集成技术

3.1 DDE信息交换的网络集成方法通过共享存储器的DDE技术为实现控制网络与信息网络的集成提供了技术支持，有很强的实时性。工程设计以工控计算机IPC作为通信处理机，该IPC机同时也是2个网络的工作站，跨接控制网络和信息网络，在沟通2个网络中起桥梁作用。通信处理机IPC用DDE方法实现2个网络间各站点的通信，是整个集成网络的关键，它能实现以下功能:(1)
搜集控制网络上各站点的实时数据信息，写入信息网络的数据库，以便信息网络用户浏览、查询;(2) 将信息网络用户的控制信息及时下达至控制网络的指定工作站点。基于通信处理机DDE信息交换的网络集成方法如图3所示。

图3 基于通信处理机DDE信息交换的网络集成方法

3.2 组态软件iFix与VB之间的DDE实现现场总线控制系统采用Inbbblution公司开发的组态软件iFix2.2作为SCADA监控操作平台。iFix是一种工业自动化组态软件，它采用图形用户界面，提供了监控和数据采集功能,为操作人员和开发人员提供了良好的监控环境，可以实现对象自由组态及动态属性的在线配置、现场动态数据采集、数据处理、状态监控、报警、参数设置、报表生成、数据存储、接口等基本功能和网络管理功能。在各种操作系统上的版本共享相同的内核，允许在同一网络结构中运行建立在不同操作系统上的iFix版本。iFix包含大量图形工具，使用户能够快速地开发系统，而且它提供了强大的功能，包括实时过程的监视和监督控制、报警和报警管理、历史趋势，统计过程控制、基于用户的安全系统、方便的系统扩展、网络功能等。而VB6.0是微软公司推出的一个流行且强大的快速开发工具,在开发SCADA系统时，利用DDE技术把两种工具有效的结合起来，更能发挥它们各自的优势，可以获取令人满意的结果。系

统分为监控子系统、数据采集子系统和数据交换子系统。以台湾磐仪工控机IPC1作为SCADA监控硬件平台。监控计算机通过挂在CC-bbbb总线上的远程I/O模块和数据采集模块，即采集子系统与现场的监控仪表相联系。采集子系统负责将现场各智能仪表采集的数据采集上来;监控系统通过DDE方式与采集子系统相联系，将现场的各种运行参数实时显示出来;监控系统根据需要给出控制命令，由采集子系统传达给挂在CC-bbbb总线上的CC-bbbb主控PLC，PLC负责现场各种设备的控制。数据交换子系统通过DDE方式与监控子系统系统交换数据，将现场实时信息经由控制网络传达到信息网络。某车间监控层过程实时数据流向如图4所示。iFix软件提供了强有力的DDE客户和服务器支持。DDE客户支持允许把来自其他应用。程序的信息传递到iFix软件中，用于数据库和画面;服务器支持允许把iFix软件的过程信息传递到其他应用程序中去处理。

图4 VB作为服务器、iFix 作为客户的数据流向图(1)
DDE客户支持iFix软件DDE客户支持允许读写DDE地址，利用DDE I/O驱动器和块配置的DDE地址，可以在过程数据库中插入来自其他应用程序、DDE驱动程序或另一个SCADA节点的数据信息。数据库中的这些信息可以按照以下方式使用:在链中传送数据、对DDE数据进行报警和用DDE数据制作趋势曲线。DDE客户支持允许在 iFix 画面中直接使用DDE，而不使用数据库中的点。即DDE可以直接应用于数据链接、动态特性(前景颜色、边界颜色、X和Y坐标、水平或垂直填充、可见性等)设置、X/Y绘图、棒状图和命令语言。iFix作为客户DDE的地址语法为:=Application|Topic|Item例如现场设备点DO1的I/O地址=VBServer|bbbb1|Text1，其中VBServer为VB开发的应用程序名，bbbb1为主题名，Text1为项目名。(2) DDE服务器支持iFix软件作为服务器允许将它的实时数据或历史数据传送到其他DDE客户应用程序中。使用iFix DDE服务器功能，需要首先启动DDE服务器程序，即iFix软件的安装目录 iFix32下的DMDDE.exe。iFix 作为服务器提供的DDE编址语法如表1所示。3.3 VB的DDE链接属性VB作为bbbbbbs环境下非常流行的快速开发工具，与bbbbbbs操作系统同出于微软一家，它理所当然地支持bbbbbbs下的DDE技术。用VB可以方便快捷地开发出DDE客户或服务器的应用程序。(1)
VB的DDE属性、DDE事件和DDE方法VB中支持DDE的对象有5类:窗体(bbbb)、多文档窗体(MDI bbbb)、标签(Label)、文本框(TextBox)和图片框(PictureBox)。其中，窗体和多文档窗体可作为DDE服务器即数据的提供者，Label、TextBox和PictureBox等可以作为DDE服务器即数据的接收者。VB为支持DDE给发送端对象提供了2种DDE属性和4种DDE事件，给接收端对象提供了4种DDE属性、4种DDE事件和4种DDE方法(见表2)。(2) 利用VB开发DDE客户/服务器应用程序在利用VB开发DDE客户/服务器应用程序中，欲建立DDE链接，完全依赖对象的DDE属性设置。VB分别作为DDE客户和DDE服务器时，DDE属性的不同设置(见表3)。(3) 动态数据交换的过程DDE管理器作为服务端通过驱动程序从PLC的内存中采集到数据，与组态进行数据交换后又通过驱动程序写入PLC的内存区，这一过程的示意图如图5所示。

图5 动态数据交换的实际过程

(4) 动态数据交换的建立过程DDE工程的建立主要包括PLC细节的描述、网络的设置、数据点的选取，其中主要是进行设备的配置和点的设置。接下来建立需要监控的点，并对其进行编辑，包括:定义监控点的名字、PLC的类型、监控点在PLC内存中的位置、数据的类型等。可根据PLC机架上输入输出单元的点数来定义输入字和输出字，同时定义手动/自动控制标志位。3.4 VB作为DDE服务器、iFix 作为DDE客户的实际链接有些参数需要通过VB开发的应用程序VBServer把从远程现场采集的实时数据传输到iFix实现显示或制作趋势图，如油漆烘间的实测温度、纯水进口压力、循环水过滤器压力、颜料的实测浓度、电泳循环泵的转速和胶炉实测温度、一次抽风系统增压机的进口和出口压力、空气预热器蒸汽温度等参数。在VBServer中，把采集到的实时数据赋给TextBox(文本框)，并把iFix中各点的DDE地址的项目名设为对应的TextBox(文本框)。如油漆烘间的实测温度，在iFix中点名为AI_Oven_Tem,其DDE地址VBServer|bbbbMain|txt OvenTem(其中VBServer是应用程序名，bbbbMain是作为主题的窗体名，txtOvenTem是作为项目的文本框名称)。此时，iFix为客户，VB应用程序为服务器。3.5 VB作为DDE客户与DDE服务器iFix的实际链接通常情况下，现场的检测信号和运动参数的流向是从iFix传输到VB开发的应用程序VBSrvApp或其它的bbbbbbs应用程序，再由bbbbbbs应用程序或VBSrvApp以命令形式经iFix下达给远程现场的智能仪表或PLC等远程的现场设备，如油漆烘间和胶炉各自的设定温度、纯水进口的设定压力、颜料的设定浓度等参数。在VBServer中，把各个设定参数相应的TextBox(文本框)的bbbbItem属性设置为对应的iFix的点，然后把从iFix的点传输到对应TextBox(文本框)中的内容下达给远程现场设备。此时，VB应用程序为VBServer客户，iFix

为服务器。