分类号_____ 密级 公开

UDC 注 1_____

学 位 论 文

西门子工业控制网络技术研究与应用

（题名和副题名）

陈 建
（作者姓名）

指导教师姓名 姜建芳 教 授

申请学位级别 硕 士 专业名称 控制理论与控制工程

论文提交日期 2005.6 论文答辩日期 2005.7

学位授予单位和日期 南京理工大学

答辩委员会主席_____

评阅人_____

2005 年 6 月 26 日

注 1：注明《国际十进分类法 UDC》的分类号。

摘 要

工业控制网络技术在当今自动化系统中发挥着越来越重要的作用。本文是以某高校西门子工业控制网络实验室建设为背景展开研究的。论文研究了西门子工业控制网络中的MPI多点通信技术和PROFIBUS现场总线通信技术，探讨了PROFInet工业以太网技术特点与应用前景。实现了基于MPI通信协议的多种通信方式，归纳出它们的不同之处与适用条件；总结出应用STEP 7软件判断CPU是否能进行基于PROFIBUS-DP协议的DX通信的方法。研究了OPC应用程序接口标准的原理，总结了它在西门子工业控制网络中的一般应用方法与系统结构。对基于PC的自动化产品WinAC系统的组成及其软件接口进行了研究与应用，探讨了它与传统的硬PLC的异同。由于无论软PLC系统还是传统的硬PLC系统，控制系统的可靠性都是需要考虑的重要问题，因此最后研究了S7-300系统软冗余技术，并给出了若干设计注意点。

本文对上述内容进行了研究、探讨与应用，并设计了若干实例，对相关设计方法进行了总结。

关键词：MPI通信协议，PROFIBUS现场总线，WinAC，工业以太网，OPC接口，冗余技术

ABSTRACT

Industrial control network technology plays an important role in automation systems nowadays. This paper is based on a project of a university constructing a laboratory on SIMATIC industrial control network. Here, technology of MPI(Multi-Point Interface) communication and PROFIBUS communication are researched, and the technological characteristics and the prospect of applying PROFInet are discussed. Also, several methods of communication based on MPI protocol are realized, and their differences and conditions for applying them are concluded. A method to judge a CPU whether it suppots DX communication based on PROFIBUS-DP protocol is also given clearly. The principle of OPC interface criterion for applications is researched, and normal applications and stuctures of different systems are conclued in SIMATIC industrial control network. Contents of WinAC system which is a automation product based on PC and its software interfaces are researched and applied. At the same time, similarities and differences between WinAC and traditional hardware-PLC are discussed. As the dependability of control systems is an important factor need to be considered in either soft-PLC systems or traditional hardware-PLC systems, technology on software-redundancy of S7-300 systems is studied, and some suggestions on designing those systems are also given.

In this paper, those technologies above are researched and discussed, and a number of sample systems are designed to apply them, and relative methods are concluded.

KEY WORDS: MPI communication protocol, PROFIBUS fieldbus, WinAC, Industrial Ethernet, OPC Interface, Redundancy technology

声　明

本学位论文是我在导师的指导下取得的研究成果，尽我所知，在本学位论文中，除了加以标注和致谢的部分外，不包含其他人已经发表或公布过的研究成果，也不包含我为获得任何教育机构的学位或学历而使用过的材料。与我一同工作的同事对本学位论文做出的贡献均已在论文中作了明确的说明。

研究生签名：陈建　　2005年6月20日

学位论文使用授权声明

南京理工大学有权保存本学位论文的电子和纸质文档，可以借阅或上网公布本学位论文的全部或部分内容，可以向有关部门或机构送交并授权其保存、借阅或上网公布本学位论文的全部或部分内容。对于保密论文，按保密的有关规定和程序处理。

研究生签名：陈建　　2005年6月20日

1 绪论

1.1 工业控制系统概论

工业控制系统其实从20世纪40年代就开始使用了，采用只具备简单测控功能的现场基地式气动仪表，即第一代过程控制系统（直动式或PCS）。气动控制一直沿用到20世纪60年代才结束它的主导地位，而在一些特殊的场合仍然发挥着不可替代的作用，如防爆场所。

接着，4～20mA模拟信号标准使得模拟控制延续了25年，即第二代过程控制系统（模拟式或ACS），但是，并非所有的传感器和执行器都使用相同的信号，大量仪器仪表使用其它类型的信号，这限制了控制系统的规模和性能，增加了系统集成的难度。

70年代，数字计算机在测量、模拟和逻辑控制领域被广泛使用，从而产生了集中式控制，即第三代过程控制系统（CCS）。它采用单片机、PLC或微机作为控制器，控制器内部传输的是数字信号，因此克服了模拟仪表控制系统中模拟信号精度低的缺陷，提高了系统的抗干扰能力，易于根据全局情况进行控制计算和判断，在控制方式、控制时机的选择上可以统一调度和安排。但集中式计算机控制系统可靠性低，集中控制把危险也集中了，一旦计算机发生了故障，将导致生产全面瘫痪。

1975年，美国Honeywell公司首先发明了以微处理器为基础的TDC2000集散型控制系统，即第四代过程控制系统（DCS）。其核心思想是集中管理、分散控制，这种分布式的控制系统体系结构有力地克服了集中式数字控制系统中对控制器处理能力和可靠性要求高的缺陷，因此，DCS在冶金、电力、石油、化工、轻工等工业过程控制应用中得到迅猛发展。但是不同的DCS厂家为了达到垄断经营的目的而对其控制通信网络采用各自专用的封闭形式，不同厂家的DCS系统之间以及DCS与上层Intranet、Internet信息网络之间难以实现网络互联和信息共享，因此集散控制系统从这个角度而言实质上是一种封闭专用的、不具有可互操作性的分布式控制系统。

80年代后期以来，随着控制、计算机、通信、网络等技术的飞速发展，自动化工业控制系统结构发生了深刻的变革，逐步形成以网络集成自动化为基础的企业信息系统。这是一种新型的、开放的、数字化的、容易进行数据交换的工业控制系统，即现场总线控制系统（FCS）。按IEC和现场总线基金会的定义，现场总线是连接智能现场设备和自动化系统的数字式、双向传输、多分支结构的通信网络。现场总线不仅是当今3C技术（Computer、Control、Communication）发展的结合点，也是过程控制技术、自动化仪表技术和计算机网络技术发展的交汇点，是信息技术、网络技术的发展在控制领域的集中体现，是信息技术、网络技术延伸到现场的必然结

果。

现场总线技术作为一种网络通信技术经过几十年的发展，国际上出现了几个具有代表性的现场总线标准[3][9]：

（1）基金会现场总线（Foundation Fieldbus）

在现场总线标准的研究制订过程中，出现过多种企业集团或组织，通过不断的竞争，到1994年在国际上基本上形成了两大阵营，一个以Fisher-Rosemount公司为首，联合Foxboro、横河、ABB、西门子等80家公司制订的ISP协议；另一个以Honeywell公司为首，联合欧洲150家公司制订的World FIP协议。这两大集团于1994年合并，成立现场总线基金会(Fieldbus Foundation,FF)，致力于开发国际上统一的现场总线协议。

（2）PROFIBUS现场总线

PRORIBUS是Process Fieldbus的缩写,是一种国际性的开放式现场总线标准,目前世界上许多自动化生产厂家都为它们生产的设备提供PROFIBUS接口。它是作为德国国家标准和欧洲国家标准的现场总线标准。该项技术是由西门子公司为主的十几家德国公司、研究所共同推出的，目前占据了现场总线市场的相当份额。

（3）LonWork现场总线(Local Operating Network：局部操作网)

它是由美国Echelon公司于1990年正式推出的。它采用ISO/OSI模型的全部七层协议，采用了面向对象的设计方法，通过网络变量把网络通信设计简化为参数设置，其最大传输速率为1.5Mbps,传输距离为2.7km，传输介质可以是双绞线、光缆、射频、红外线和电力线等。

（4）CAN总线(Control Area Network：控制局域网)

最早由德国BOSCH公司推出，用于汽车内部测量与执行部件之间的数据通信。CAN结构模型取ISO/OSI模型的第一、二、七层协议，即物理层、数据链路层和应用层。

（5）HART总线（Highway Addressable Remote Transducer：可寻址远程传感器数据公路）

它是由美国Rosemount公司最早推出的一种兼容4～20mA模拟信号和调制数字信号的现场总线协议。其数字通信由于采用调制/解调方式，属于模拟系统向数字系统转变过程中的过渡产品。

（6）PROFInet

PROFInet源自PROFIBUS现场总线国际组织（PI）的开放的自动化总线标准，是新一代基于以太网技术的工业通信解决方案。它实现了从现场控制层到管理层的无缝集成，并提供一个开放的基础构架。

现场总线不单单是一种通信技术，它有效地实现了智能仪表、通信网络和控制

系统的集成，其本质原理和技术特征集中表现在：

（1）现场通信网络，实现过程控制、加工制造现场仪表或设备的现场数字化通信。

（2）现场设备互连，仅仅用一对传输线（如双绞线、同轴电缆、光纤或电源线等）将传感器、变送器和执行器等现场仪表和设备互连起来。

（3）互操作性，在遵守同一通信协议的前提下，现场总线允许选用各制造商性能价格比最高的产品集成在一起，实现对来自不同厂商的设备的互相连接、统一组态。

（4）功能分散，将控制功能分散到工业控制现场，因此现场仪表多为智能型多功能仪表。

（5）通信线供电，对于本质安全要求的低功耗现场仪表，允许直接从通信线上摄取能源。

（6）开放式互连，现场总线作为开放式互联网络，既可与同层网络互连，也可以通过网络互联设备与不同层次的控制级网络和信息级网络互联，共享资源，统一调度。

因此，现场总线控制系统既是一个开放的通信网络，又是一种全分布控制系统，它作为智能设备的联系纽带，把挂接在总线上作为网络节点的智能设备连接为网络系统，并进一步构成自动化系统。它在制造业、流程工业、交通、楼宇等方面的自动化系统中具有广泛的应用前景。

随着 FCS 的不断推广，近几年出现了一种新型的自动化系统控制策略，即由工业计算机（工业 PC）、I/O 装置、监控装置、控制网络等组成的基于 PC 的控制系统（PCBCS），它正迅速进入工业控制领域，成为实现低成本工业自动化的重要途径。PCBCS 控制系统的优点可概括为：对各种控制及业务应用、信息的存取均很简单；软件向新的硬件平台的可移植性优良；控制、人机界面及编程功能易于集成；易于将过程控制、逻辑控制、批量控制以及运动控制等合为一体；不依赖于各种专有的控制系统。目前，采用 PC-Based Control 控制思想的产品比较多，如：SIEMENS WinAC 基本型(Basis)/实时型(RTX)/插槽型(Slot)，WinCAT，Visual Logic Controller，SoftLogix，FactorySuite/InControl，PARADYM-31 等。

目前，工业控制系统正向智能化、网络化和集成化方向发展，形成了功能强大的工业控制网络，实现了设备的大规模互联，此外性能优越的基于网络的交互式控制、触觉控制、声音输入等技术也被引入了控制网络，使人们可以随时随地以多种途径参与自动化系统控制和管理。因此，21 世纪工业控制系统将是一个网络化的、全集成自动化（Totally Integrated Automation，TIA）的全方位的一体化系统，必将在全球范围内带来新的变革！

1.2 西门子工业控制网络体系

一般地，企业通信网络可分为三级：企业级、车间级和现场级。企业级通信网络用于企业的上层管理，为企业提供生产、经营、管理等数据，通过信息化的方式优化企业的资源，提高企业的管理水平。在这一层通信网络中，IT 技术应用十分广泛，如 Internet/Intranet、IP 技术等。车间级通信网络介于企业级和现场级之间。它的主要任务是解决车间内需要协调工作的不同工艺段之间的通信，要求通信网络能够高速传递大量信息数据和少量控制数据，同时具有较强的实时性。现场级通信网络处于工业网络系统的最底层，直接连接现场的各种设备，如 I/O 设备、传感器、变送器、变频与驱动等装置。这一层通信网络上主要传递控制信号，对网络的实时性和确定性有很高要求。

作为全球领先的自动化系统提供商，德国西门子公司提供了非常完整的工业控制通信方案 SIMATIC NET，它同样遵循三级网络构架结构。下面将阐述其总体构架和技术内涵。

1.2.1 西门子工业控制网络总体构架

西门子工业控制网络是一个覆盖了全厂范围的通信网络，对全厂信息统一采集和管理，网络结构如图 1.2.1.1 所示。它主要由工业以太网（IEEE 802.3、802.3u）、工业移动通信、PROFIBUS（IEC 61158/EN 50170）、AS-i（Actuator-Sensor Interface）、EIB（European Installation Bus）总线等构成[12][13][21]。

（1）AS-i 总线

AS-i 接口是开放的国际标准 EN50295，用于现场级小数据量（主要是开关量）的传送。AS-i 规范描述了主机和主机之间的通信协议以及主机和周围设备同整个系统的连接方式，任何 AS-i 模块的生产商都遵循这些规范，保证 AS-i 产品的兼容性。

（2）EIB 总线

欧洲安装总线（European Installation Bus, EIB）是一种专门用于智能建筑领域的现场总线标准，具有分布性、开放性、互操作性和灵活性的特点。可通过编程改变 EIB 总线上智能化元件的功能，既可独立完成诸如开关、控制、监视等工作，也可根据要求进行不同的组合。与传统安装方式相比，EIB 总线的应用使元件功能增强，具有高度的灵活性。它的开放性更使得不同公司开发的基于 EIB 协议的电气设备可以完全兼容。

（3）PROFIBUS 现场总线

现场总线 PROFIBUS 是国际标准 IEC61158 的组成部分 Type III，它定义了串行现场总线系统的技术特征。串行现场总线可以从现场级到单元级使分散的数字可编程的控制器形成网络。根据其应用特点，PROFIBUS 分为：PROFIBUS-DP、PROFIBUS-FMS 和 PROFIBUS-PA 三个兼容版本。PROFIBUS 不仅适用于工厂自动化和过程自动化领域

（如化工等），而且也适用于交通工程、发电和输配电等领域。

（4）工业以太网 PROFInet

PROFInet 是基于 IEEE 802.3（Ethernet）的强大的区域和单元网络，是国际标准 IEC61158 的重要组成部分。PNO(PROFInet 组织)于 2001 年 8 月发表的 PROFInet 规范，是用于 PROFIBUS 纵向集成的、开放的、一致的综合系统解决方案。PROFInet 将工厂自动化和企业信息管理层 IT 技术有机地融为一体，同时又完全保留了 PROFIBUS 现有的开放性。PROFInet 特别重视有关保护投资的要求，以确保现有系统继续运行，同时还要求现有的系统可以集成已经安装的系统。

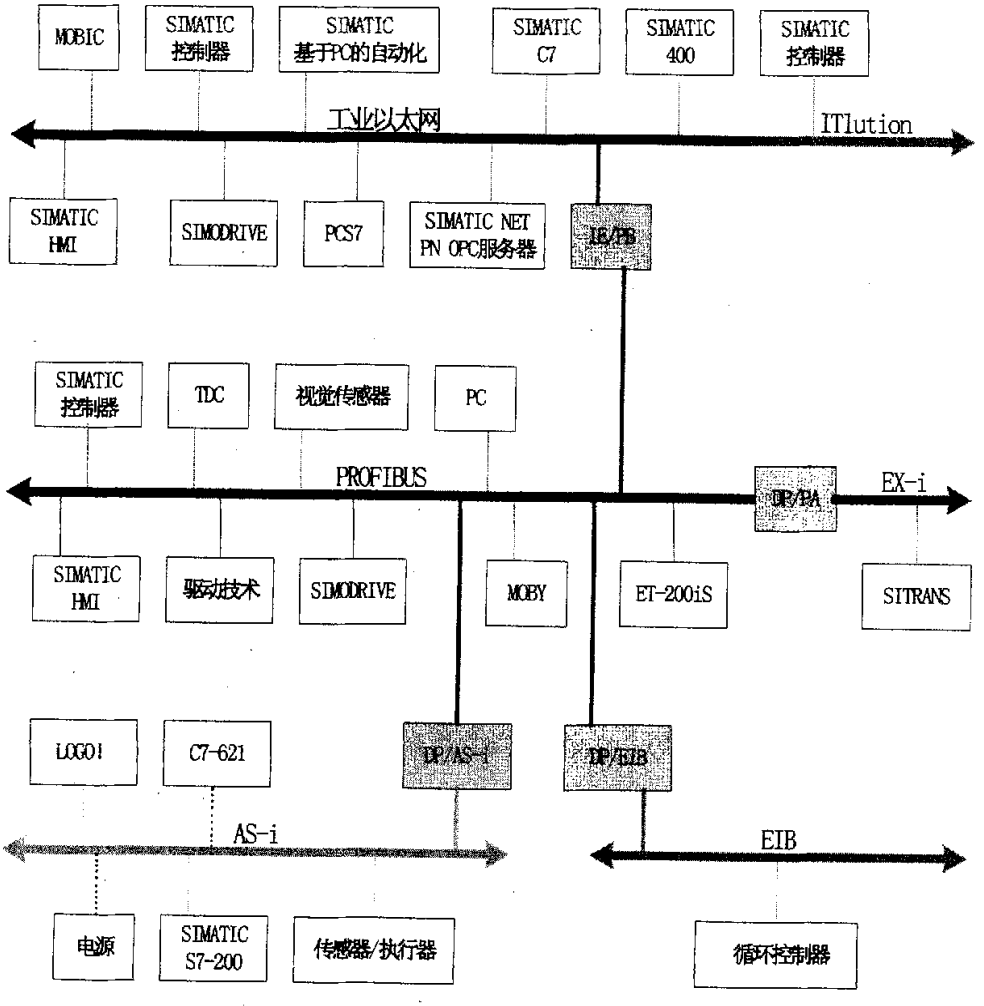


图 1.2.1.1 西门子工业控制网络总体构架

1.2.2 西门子工业控制网络技术内涵

西门子工业控制网络技术内涵丰富，大致包含如下部分：

（1）现场总线技术。适用于不同场合的现场总线如工业以太网、PROFIBUS、

AS-I、EIB，构成了西门子工业控制网络的骨架。

（2）控制网络扩展技术。控制区域规模扩大时，需要在同种或者异种控制网络之间互联，扩大信息传输范围。如MPI、PROFIBUS网络通过中继器可延伸其通信长度；应用IE/PB耦合模块可实现工业以太网与PROFIBUS网络之间的连接；DP/PA耦合模块可实现从DP总线到PA总线的过渡，将控制网络扩展至安全防爆区域；DP/AS-i耦合模块使传感器/执行器与DP总线交换数据；DP/EIB模块则使楼宇自动化信息传递到DP总线。

（3）接口技术。西门子工业控制网络是规范化的开放式控制环境，只要设备生产商或者系统集成商遵循既定的标准，就可方便地将第三方设备或第三方软件集成到控制网络中。例如，使用PROFIBUS通信专用ASIC芯片可开发出符合PROFIBUS协议规范的总线产品，满足特定的控制要求。再如，作为西门子公司与微软公司强强联合的结晶，监控软件WinCC V6.0提供C脚本和Visual Basic脚本编程接口、OLE和ActiveX接口；其软PLC产品WinAC则提供相应的ODK支持C/C++开发接口以及OPC（OLE for Process Control）接口。上述软硬件接口增强了控制网络的功能，以完成多样化的控制任务。

（4）控制网络通信技术

西门子工业控制网络中的通信技术有：MPI通信、PROFIBUS通信、以太网通信、AS-i通信、串口通信、PPI通信等。

（5）控制网络诊断技术

控制网络中诊断技术的应用可缩短安装调试周期，对于系统维护也起着举足轻重的作用。通过专用于诊断的硬件设备如BT200、诊断中继器等，以及相关具有诊断功能的软件如STEP 7、相关的功能块（FB）可实现西门子工控网络的诊断。

（6）控制网络冗余技术

在系统的可靠性要求比较严格的领域，需要对关键部分进行冗余设计，从而保障系统不间断运行。软件冗余技术和硬件冗余技术是西门子工控网络中的两个重要的冗余技术。

（7）控制网络安全性

当今Internet互联网络中存在不同程度的安全隐患，如计算机病毒、黑客，对信息安全性提出了挑战。同样，工业现场控制网络中传递的信息也存在这样的问题，如从工业以太网连接到局域网或者Internet时，未经加密的工业过程数据则有可能被窃取、破坏等。而工业过程数据一旦加密/解密，则传输速率将会降低，因此，安全性和快速性是一对矛盾。

（8）其它网络技术

其它网络技术还有：无线网络、光纤网络等相关技术。

1.3 论文作者所做的主要工作

论文作者以某高校西门子工业控制网络实验室建设项目为背景，所做的主要工作包括以下几个方面：

（1）研究了西门子工业控制网络体系结构，总结了蕴含于其中的技术内涵，并选取了其中的几项技术进行了深入研究。

（2）对西门子工业控制网络中的若干通信技术如 MPI、PROFIBUS、PROFInet 通信技术特点进行了研究和总结。

（3）研究了 MPI 的三种通信方式：全局数据包通信方式、无组态连接通信方式、组态连接通信方式，并利用实验室现有的软硬件，实现了前二者通信方式，对其适用场合与使用条件进行了比较。

（4）研究了 PROFIBUS-DP 通信、FDL 通信、DX 通信，对各自特点进行了比较，并总结出应用 STEP 7 软件判断 CPU 是否能进行 DX 通信的方法；

(5)设计了一个 S7-200 与 S7-300 之间的 PROFInet 通信网络，给出了 PROFInet 网络配置的详细方法，并探讨了 PROFInet 的应用前景。

（6）对 OPC 接口技术进行了研究，分析了它在 SIMATIC NET 中的应用，重点研究了 OPC 在 S7-200 系统、S7-300 系统以及 HMI（Human Machine Interface）中的应用。

（7）研究了 OPC 的 DCOM 配置，并应用 OPC 技术设计了基于 S7-200 系统的配方系统，重点研究了应用 OPC 进行监控程序开发的若干技术。编写了配方演示系统的 PLC 控制程序、基于 OPC 方式的上位机监控程序和虚拟对象程序，并比较了 OPC 技术与 Prodave、PPI 等通信方式的优劣。

（8）深入研究了基于 PC 的自动化产品 WinAC 系统的组成、典型配置，重点研究了 WinAC 系统的软件接口，如 Excel 接口、OPC 接口、C/C++编程接口等。应用上述技术，设计了基于 WinAC 的电梯群控教学系统，应用 VC++ 6.0 编写了 COM 对象，应用 MicroWin32 4.0 编写了 PLC 控制程序，应用 Protool/Pro 6.0 设计了监控程序、应用 VB 6.0 编写了基于 OPC 的虚拟电梯对象。

（9）最后，研究了西门子工业控制网络冗余技术，探讨了 S7-300 系统的软件冗余原理及其实现的条件，给出了若干注意点。

2 西门子工业控制网络中的通信技术

SIMATIC NET 控制网络中使用了许多通信技术，其中的 MPI 通信、PROFIBUS 通信以及工业以太网通信在工业现场使用率较高，本章针对它们进行了较深入的研究与探讨。

2.1 MPI 通信技术的研究与实现

2.1.1 MPI 通信技术概述

MPI（Multi-Point Interface，多点接口）通信适用于小范围的现场级通信，通信速率为 19.2Kbps～12Mbps，通常默认值为 187.5Kbps，通过 DP/MPI 接口才可支持 12Mbps 通信速率。MPI 网络最多连接 32 个节点，最大通信距离为 50m，但可通过 RS485 中继器延长 MPI 网络通信距离[8] [17][19] [21]。

S7-200/300/400 系列 CPU 上的 RS485 编程口可作为 MPI 通信口使用。PLC 之间的 MPI 通信有三种方式：全局数据包通信方式、无组态连接通信方式、组态连接通信方式。其中组态连接通信方式仅适合 S7-300 与 S7-400 或者 S7-400 之间进行通信，限于实验室硬件条件，着重对前二者通信方式进行了研究。

2.1.2 全局数据包 MPI 通信

全局数据包方式的 MPI 通信无需编程，只需组态 PLC 的发送区与接收区，适用于 S7-300、S7-400 PLC 之间的通信。作者应用 CPU 315-2DP、CPU 314C-2DP、CP 5613 通信卡、MPI 电缆、STEP 7 V5.2（西门子编程组态集成开发环境），实现了全局数据包通信。

（1）通信参数设置

在 STEP 7 中新建工程，并插入两个 SIMATIC 300 STATION，分别命名为 Station_315 和 Station_314C，分别进行硬件组态（HW Config），将 MPI 地址分别设置为 2 和 4，通信速率默认为 187.5Kbps 即可。

（2）组态数据发送区与接收区

通过 STEP 7 中的“Define Global Data”功能，可定义用于数据交换的地址区，如 DB、M、I、Q 区，发送区与接收区长度需一致。S7-300 CPU 支持最大 22 字节地址区，这里将 CPU 315-2DP 中 DB10 的前 22 字节发送到 CPU 314-2DP 中 DB20 的前 22 字节。编译后，每行通信区都会分配到一个全局数据包标识号 GD ID（GD X.Y.Z），组态界面如图 2.1.2.1 所示，GD ID 为“GD 1.1.1”。其中 X 表示全局数据包的循环数，与 CPU 型号有关；Y 表示全局数据包的个数；Z 表示一个数据包里的数据区数。

（3）下载配置并运行

在两站点中分别插入数据块 DB10 和 DB20，并将上述组态数据编译后下载至两

个 CPU 中（此时的 PG/PC 接口配置需设置成“S7ONLINE (STEP 7) →CP 5613_5614 MPI”），即可实现两 PLC 通信。为验证正确性，可初始化 DB10 从 Byte0～Byte21 为“B#16#0”～“B#16#15”，并在 Station_314C 站点中插入变量表 VAT1（Variable Table），在线监视 Station_315 发送的数据。图 2.1.2.2 证明了全局数据包方式通信的正确性。

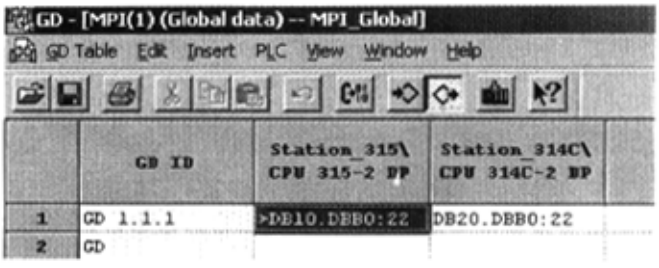


图 2.1.2.1 组态数据发送区与接收区

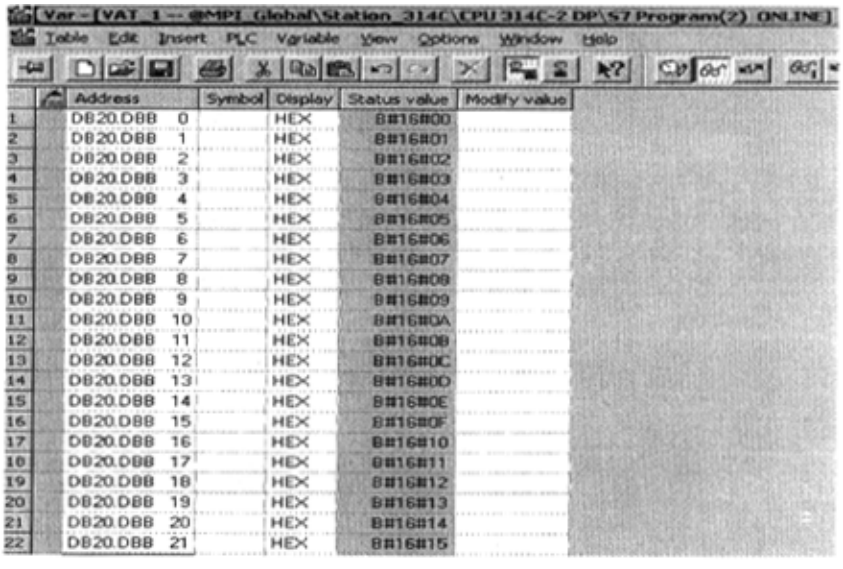


图 2.1.2.2 站点 Station_314C 中接收到的数据

组态全局数据包的长度必须与 DB 块中实际分配的变量地址长度一致，如组态了长度为 22 的发送区/接收区，则需在 DB 块中分配长度为 22 的变量区。否则，组态配置数据下载之后，CPU 虽然没有任何报错指示，但不能进行正常通信。

2.1.3 无组态连接的 MPI 通信

与全局数据包方式有所不同，无组态 MPI 通信方式则需调用相应系统功能块（SFC）实现。根据编程方式的不同，可分为单边编程通信方式和双边编程通信方式。

（1）单边编程通信方式

只需在一方 PLC（作为客户机）编程，访问另一方 PLC（作为服务器，无需编程）。该方式适用于 S7-200、S7-300、S7-400 PLC 之间的通信。

A. S7-200 与 S7-300 之间的单边编程通信

在与 S7-200 进行无组态 MPI 通信时，S7-200 CPU 只可用做服务器。作者选用了 CPU 224、EM 277（地址拨码开关设置为 4）和 CPU 314C-2DP（Station_314C）实现了单边编程通信。硬件组态时，设置 Station_314C 的 MPI 地址为 2，通信速率默认为 187.5Kbps。

在 OB1（组织功能块）中调用 SFC67（“X_GET”），当 M0.0=1 时，从 S7-200 PLC 的 VB0 得到数据并保存在本地 DB2.DBB0 中。调用 SFC68（“X_PUT”），当 M1.0=1 时，将 DB2.DBB1 中的数据发送到 S7-200 PLC 的 VB1 中。这里，对 S7-200 的 V 区访问时，需在 S7-300 中用 DB1 表示。如图 2.1.3.1 和 2.1.3.2 所示：

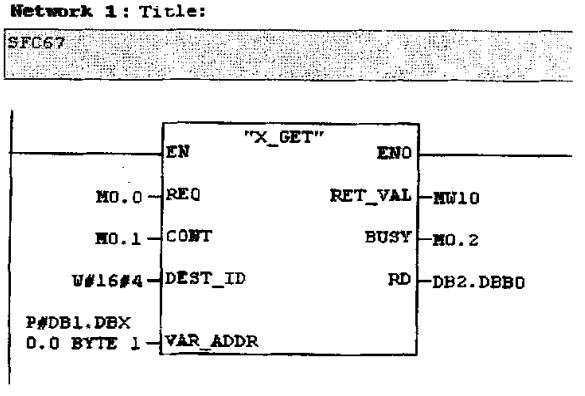


图 2.1.3.1 接收数据

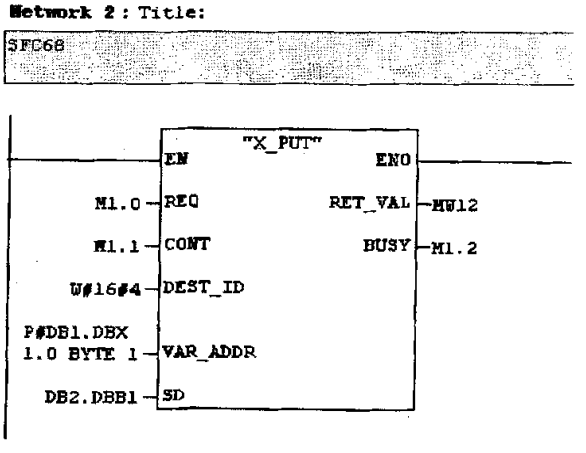


图 2.1.3.2 发送数据

系统功能块 SFC67、SFC68 参数说明：

REQ：SFC 的使能信号，BOOL 类型；

CONT：SFC“持续执行”使能信号，BOOL 类型，CONT=0 时，当数据交换结束，PLC 之间的 MPI 连接将会终止，CONT=1 时，PLC 之间的 MPI 连接将始终保持，此时需调用 SFC69 终止与对方 PLC 的 MPI 连接；

DEST_ID：对方 PLC 的 MPI 地址，WORD 类型；

VAR_ADDR：对方 PLC 的数据接收区，ANY 类型；

SD：本地数据发送区，ANY 类型；

RD：本地数据接收区，ANY 类型；

RET_VAL：错误码返回值，INT 类型；

BUSY：等于 1 表示发送/接受数据未完成，等于 0 则表示发送/接受已完成或尚未发送/接受数据，BOOL 类型。

在 DB2 中设置 DB2.DBB0 与 DB2.DBB1 的初始值为 B#16#0 和 B#16#FF。在 S7-200 PLC 的编程环境 MicroWin32 中编写程序，将 VB0 置为 100，将 VB1 的内容输出到 QB0 输出口。因此，在通信时，S7-200 的 Q0.0～Q0.7 被点亮，同时在 S7-300 中可监视如图 2.1.3.3 所示：

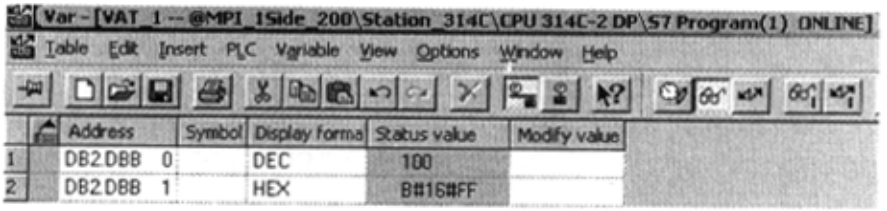


图 2.1.3.3 S7-200 与 S7-300 单边编程通信结果

证明 S7-200 与 S7-300 的单边编程 MPI 通信是成功的。

B. S7-300 PLC 之间的单边编程通信

S7-300 PLC 之间进行单边编程通信时，S7-300 PLC 的任一方均可作为客户机或服务器。作者选用了 CPU 315-2DP 做服务器（Station_315，MPI 地址设为 4）与 CPU 314C-2DP 做客户机（Station_314C，MPI 地址设为 2）实现了单边编程通信。

在 Station_315 中插入数据块 DB1，并在组织块 OB1 中编程实现：当 DB1.DBW0=200 时，则 DB1.DBW2 中的数值不断自加，直至等于 10000。

在 Station_314C 中插入 DB2，并把 DB2.DBW0 初始值设为 200。在 OB1 中应用 SFC67 接收数据，用 SFC68 发送数据，其参数说明见上文。在 Station_314C 站中可监视到 DB2.DBW2 从 200 以步长为 1 增加到 10000，如图 2.1.3.4 所示，证明 S7-300 PLC 之间的单边 MPI 编程通信是可行的。

VAT_1 -- @MPI 1Side_300\Station_314C\CPU 314C-2 DP\S7 Program(1) ONLINE

	Address	Symbol	Display for	Status value	Modify value
1	DB2.DBW 0		DEC	200	
2	DB2.DBW 2		DEC	10000	
3					

图 2.1.3.4 S7-300 PLC 之间的单边编程通信结果

（2）双边编程方式

该方式下的 PLC 通信需要对双方 PLC 调用系统功能块，适用于 S7-300、S7-400 PLC 通信。作者选用了 CPU 315-2DP（Station_315，MPI 地址设为 4），CPU 314C-2DP（Station_314C，MPI 地址设为 2）实现了双边编程方式的 MPI 通信。

在 Station_315 中，调用 SFC65，将存储在 DB1.DBW0 和 DB1.DBW2 中的两个数据发送至 Station_314C，由 Station_314C 计算这两个数据的和、差，并将该运算结果发送回 Station_315，由 Station_315 调用 SFC66 接受数据，根据数据包的标识符分拣出 Station_314C 发送的数据包，并分别存储在 DB1.DBW4 与 DB1.DBW6 中。如图 2.1.3.5、2.1.3.6 和 2.1.3.7 所示。

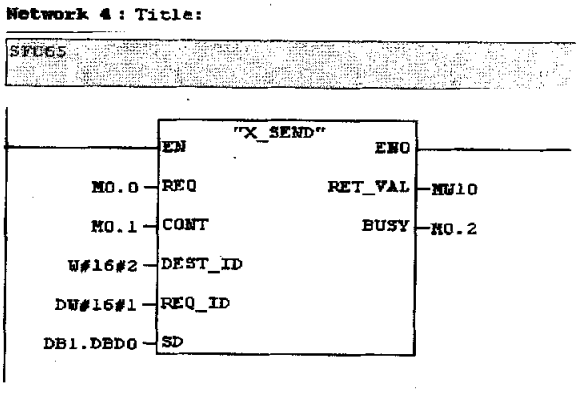


图 2.1.3.5 发送数据

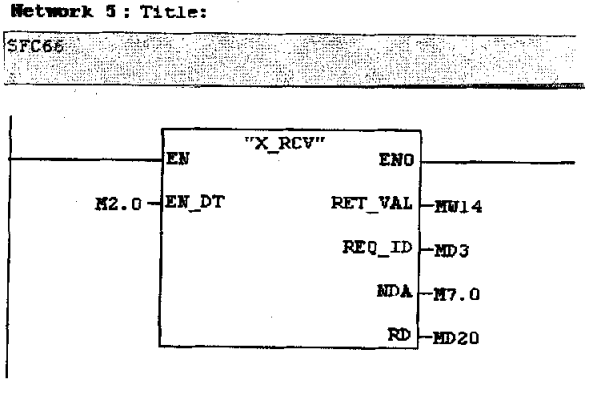


图 2.1.3.6 接收数据

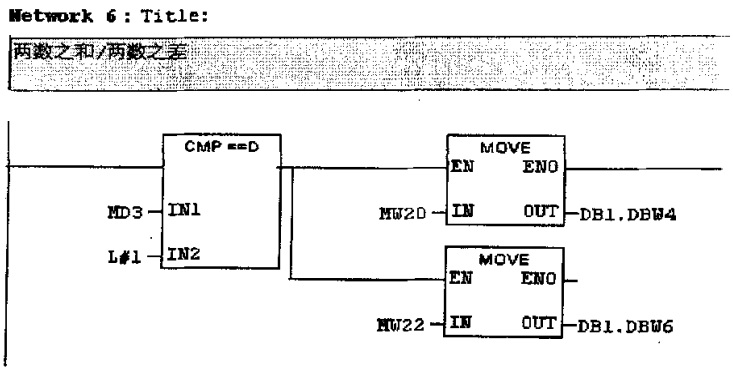


图 2.1.3.7 分拣并存储数据

SFC65 参数说明：

REQ：发送请求，为 1 是发送，BOOL 类型；

CONT：连续发送，BOOL 类型；

DEST_ID：对方 PLC 的 MPI 地址，WORD 类型；

REQ_ID：数据包的标识符，以标明不同的数据包，此处定义为“1”，DWORD 类型；

SD：数据发送区，ANY 类型；

RET_VAL：返回值，INT 类型；

BUSY：通信状态标志，为 1 时标志正在发送，为 0 时表示发送完成或未发送，BOOL 类型。

SFC66 参数说明：

EN_DT：接受使能，BOOL 类型；

RET_VAL：返回值，INT 类型；

REQ_ID：数据包标识符，DWORD 类型；

NDA：为 1 表示有新的数据包，为 0 表示没有新的数据包，BOOL 类型；

RD：数据接收区，ANY 类型。

运行结果如图 2.1.3.8 所示，Station_315 将存储在 DB1.DBW0 和 DB1.DBW2 中的两个数据发送给 Station_314C 后，由 Station_314C 计算二者的和、差后将运算结果发回到 Station_315，并分别存储在 DB1.DBW4 和 DB1.DBW6 中，证明 S7-300 PLC 间的双边编程 MPI 通信在实际应用中是可行的。

VAT 1 -- MPI 2Side\Station_315\CPU 315-2 DP\S7 Program(1) ONLINE

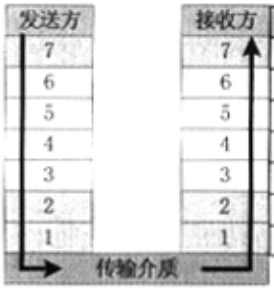
	Address	Symbol	Display forma	Status value	Modify value
1	DB1.DBW 0		DEC	180	
2	DB1.DBW 2		DEC	280	
3	DB1.DBW 4		DEC	460	
4	DB1.DBW 6		DEC	100	

图 2.1.3.8 双边编程通信结果

2.2 PROFIBUS-DP 通信技术的研究与实现

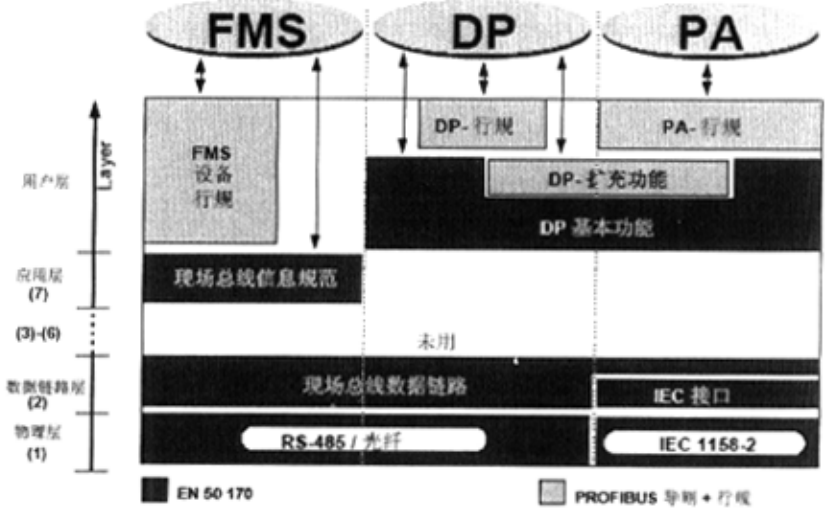
2.2.1 PROFIBUS 总线技术特点[1][6][21][24]

PROFIBUS 协议结构是根据 ISO7498 国际标准，以开放式系统互联网络(Open System Interconnection，OSI)作为参考模型的，如图 2.2.1.1 所示。现场总线采用简化的网络体系结构，如图 2.2.1.2 所示，具有类似于 OSI 模型的物理层、数据链路层和应用层的三层协议或进一步包括网络层或传输层在内的四层协议，而不采用会话层和表示层。流量控制和差错控制放在数据链路层执行，而报文的可靠传输可以放在数据链路层或者应用层执行。



各层名称	功 能
应用层	对面向应用要求的应用程序的接口（读、写）
表示层	用于下一层分析和解释的数据表达方式（编码）
会话层	建立和清除临时的站连接；通信进程的同步
传输层	为第 5 层控制数据传输（分解成数据包，出错控制）
网络层	建立和清除连接，避免网络堵塞
数据链路层	包括数据安全的总线存取协议描述(介质存取控制)
物理层	定义介质（硬件），数据编码和传输速度

图 2.2.1.1 OSI 参考模型



2.2.1.2 PROFIBUS 协议结构

PROFIBUS 提供三种通信协议类型：DP、FMS 和 PA。其中 PROFIBUS-DP 是一种经过优化的高速通信连接，专为自动控制系统和分散 I/O 设备之间通信设计，用于分布式控制系统的高速数据传输，传输速率最高可达 12Mbps；PROFIBUS-FMS 主要解

决车间级通用性通信任务，提供大量的通信服务，完成中等速度的循环和非循环通信任务；PROFIBUS-PA 专为过程自动化设计，提供标准的本质安全传输技术，用于对安全性要求较高的需要总线供电的场合。

DP 协议规定了循环数据交换所需要的基本通信功能。依据各种应用领域的特殊需求，这些 DP 基本功能已用特殊功能逐步地进行了扩展，所以现在有三种版本：DP-V0，DP-V1 和 DP-V2 可供使用，而每一种版本都有它自己专用的关键特性，版本的这种区分，主要反映了三种版本规范制定的时间顺序。版本 V0 和 V1 包含“特性”（用于实现的绑定）和选项，而 V2 仅规定了选项。

三种版本的关键内容如下：

DP-V0 提供 DP 基本功能，包括循环的数据交换，以及站诊断、模块诊断和特定通道的诊断。

DP-V1 包含依据过程自动化的需求而增加的功能，特别是用于参数赋值、操作、智能现场设备的可视化和报警处理等（类似于循环的用户数据通信）的非循环的数据通信。这样就允许用工程工具在线访问各站点。此外，DP-V1 有三种附加的报警类型：状态报警、刷新报警和制造商专用的报警。

DP-V2 包括主要根据驱动技术的需求而增加的其它功能。由于增加的功能，如同步从站模式（Isochronous Slave Mode）和从站对从站通信(DXB，Data eXchange Broadcast)等。DP-V2 也可以被实现为驱动总线，用于控制驱动轴的快速运动时序。

2.2.2 PROFIBUS-DP 数据交换原理

PROFIBUS-DP 定义了三种设备类型：

DP-从设备：指直接连接 I/O 信号的外围设备，典型的设备如输入、输出、驱动器、阀、操作面板等。

DP-1 类主设备（DPM1）：指中央控制器，它与分散的 I/O 设备（DP-从设备）交换数据。系统中允许存在若干个 DPM1，典型设备如：PLC、PC 等。

DP-2 类主设备（DPM2）：指组态、监视或工程工具，用于设定网络或参数，及监视 DP-从设备。PROFIBUS-DP 单主系统由 1 个 DP-DPM1 设备和 1～125 个 DP-从设备组成，而多主系统由多个 DP-DPM1 设备或 DP-DPM2 设备及最多 124 个 DP-从设备组成，即同一总线上最多 126 个设备。

PROFIBUS-DP 通信是一个主站依次轮询从站的通信方式，即 MS（Master-Slave）方式。DP-主设备与 DP-从设备交换数据时，遵循如 2.2.2.1 所示应答机制：

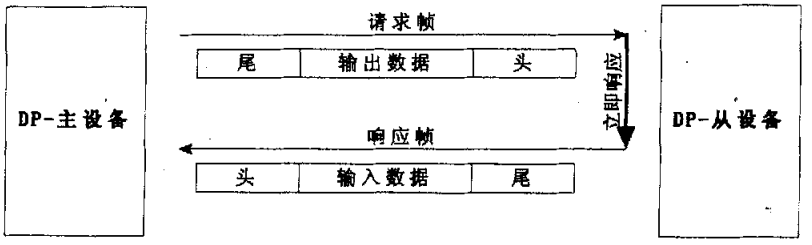


图 2.2.2.1 DP 主从设备应答机制

数据帧结构如图 2.2.2.2 所示：

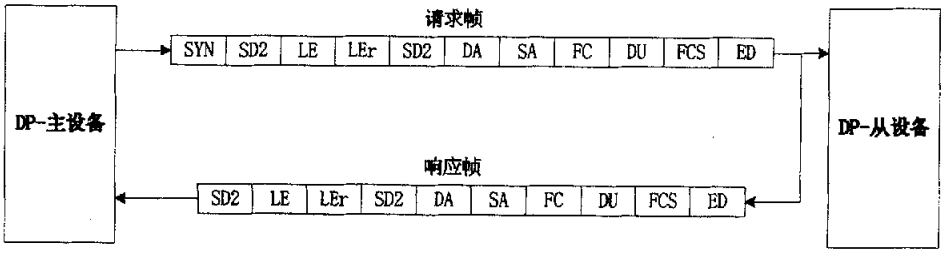


图 2.2.2.2 DP 主从设备应答数据帧

其中，SYN=同步时间，SD2=开始分界符 2，LE=长度，LEr=重复长度，DA=目的地址，SA=源地址，FC=功能码，DU=数据单元，FCS=帧检查顺序，ED=结束分界符。

2.2.3 基于 PROFIBUS-DP 的 DX 通信

基于 PROFIBUS-DP 协议的 DX（Direct data eXchange）通信模式是在主站轮询从站时，从站除了将数据发送给主站，同时还将数据发送给在 STEP 7 中组态的其它从站，无需再在主站中编写通信和数据转移程序。通信示意图如 2.2.3.1 所示：

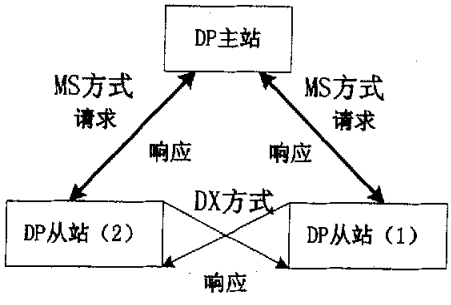


图 2.2.3.1 DX 通信示意图

基于 PROFIBUS-DP 协议的从站之间进行 DX 通信的必要条件是：系统中至少需要一台 PROFIBUS 一类主站；从站要有数据发送给主站，即从站要有输出区对应主站的输入区，并且从站是智能从站（如 S7-300 站、S7-400 站、ET200S 站、ET200X 站等），旧版本的从站或主站则不支持 DX 通信。

通过实践，作者总结出如下规律以判断 CPU 是否支持 DX 通信：能够在 STEP 7 中进行 DX 通信组态的 CPU 支持 DX 通信，否则不支持 DX 通信。如 CPU 314C-2DP 做

主站（站名：Station_314C，DP 地址为 4），CPU 315-2DP（站名：Station_315，DP 地址为 2）和 CPU 313C_2DP（站名：Station_313C，DP 地址为 3）分别做两个从站。

在 DX 通信组态之前，先要进行 MS 通信组态：新建 S7-300 站点 Station_315，不妨将订货号为 6ES7 315-2AF01-0AB0 的 CPU 315-2DP 插入机架（RACK），并新建 PROFIBUS-DP 连接，选择从站模式，默认诊断地址值，然后选择新建配置，进行 PROFIBUS-DP 属性的设置，如图 2.2.3.2 所示。

对 CPU 313C-2DP 从站（Station_313C）的设置与 Station_315 相似，只需将主站（Station_314C）输入区起始地址改为 10。设置主站 Station_314C，将 Station_315 和 Station_313C 连入 PROFIBUS-DP。硬件组态如图 2.2.3.3 所示。

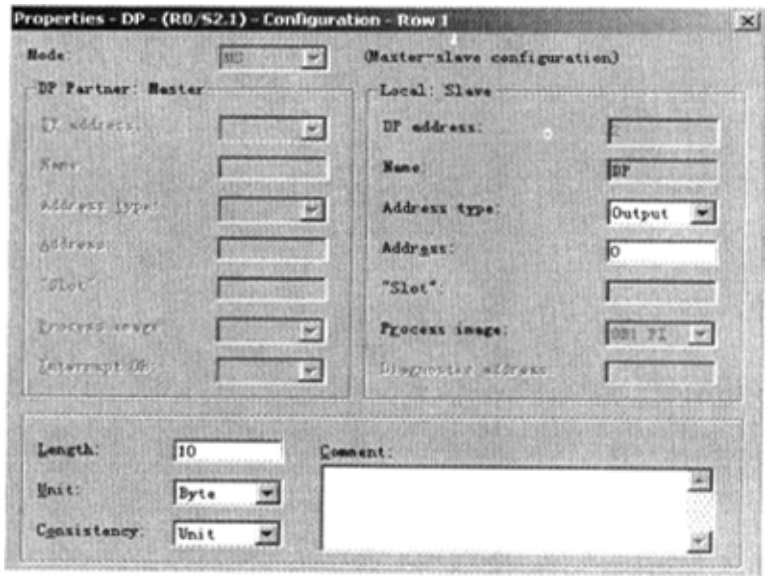


图 2.2.3.2 DP 属性设置

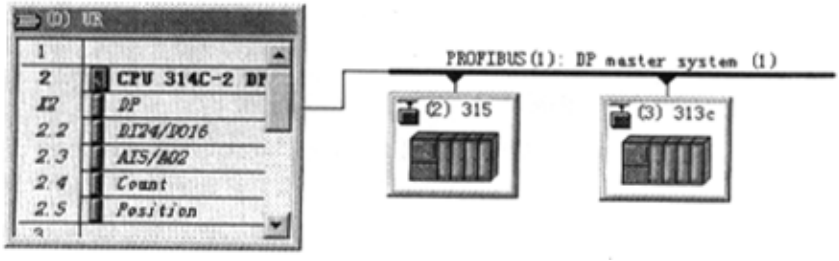


图 2.2.3.3 站点 Station_314C 硬件组态

编辑从站 Station_315 的 DP slave 属性，分配主站与它的数据交换区如图 2.2.3.4 所示。

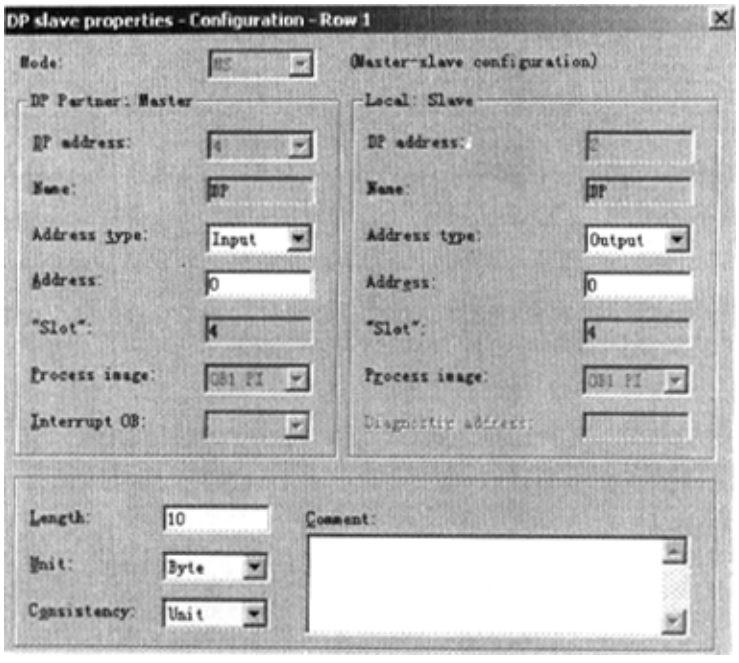


图 2.2.3.4 从站 Station_315 的 DP 属性设置

Station_313C 的 DP 从站编辑同 Station_315。至此，MS 通信模式组态完毕，也只有上面的工作完成之后才能进行 DX 通信模式的组态。

在组态 DX 通信模式时就能判断 CPU 是否支持 DX 通信。分配站点 Station_313C 的 DX 通信区，如图 2.2.3.5 所示，此时 DX 方式是不可选的。

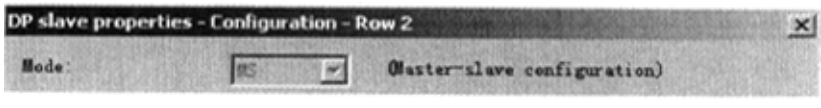


图 2.2.3.5 DX 方式不可选

若将该型号的CPU 315-2DP换成订货号为6ES7 315-2AF03-0AB0的CPU 315-2DP，则 DX 方式是可选的，如图 2.2.3.6 所示。

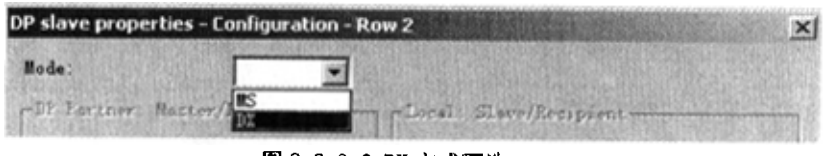


图 2.2.3.6 DX 方式可选

选择 DX 方式后，可定义从站间 DX 通信区，如图 2.2.3.7 所示。

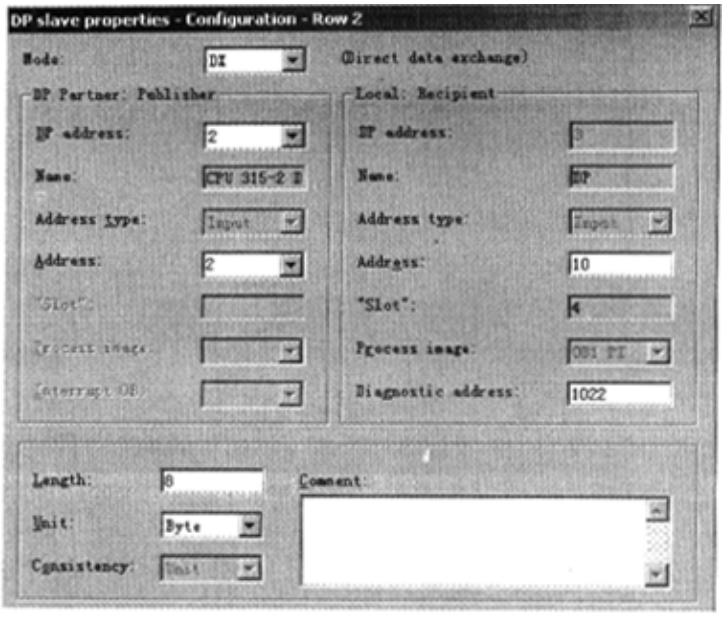


图 2.2.3.7 分配 DX 通信区

至此，DX 通信组态完毕！当 Station_314C 轮询 Station_315 时，Station_315 发送 QB0～QB9 至 Station_314C 的 IB0～IB9，同时发送 QB2～QB9 共 8 个字节至 Station_313C。

由上述过程可见，通过 STEP 7 组态可知，订货号 6ES7 315-2AF03-0AB0 对应的 CPU 是支持 DX 通信的，而订货号为 6ES7 315-2AF01-0AB0 的 CPU 不支持 DX 通信。这种方法对于同类问题也具有一般性意义。

2.2.4 基于 PROFIBUS-DP 的 FDL 通信

FDL（Fieldbus Data Layer）即数据链路层，它是 PROFIBUS 的第二层，采用混合介质存取方式，即主站间按令牌方式，主站和从站间按主从方式工作。令牌是一条特殊的电文，它在主站之间按照地址的升序传递总线控制权（即令牌），得到令牌的主站可在一定的时间内执行本站的工作。这种方式保证了在任一时刻只能有一个站点发送数据，并且任一个主站在一个特定的时间片内都可以得到总线操作权，这就避免了在同一时刻多站对总线操作的冲突。链路层保证损坏或掉电的站点从环中排除，新上电的主站加入令牌环。链路层的另一个主要任务是保证数据的无差错传输，按照国际标准 IEC870-5-1 制定的特殊的起始和结束界定符、每个字节的奇偶校验和每条电文的 CRC 循环校验保证的。从而 FDL 层的通信可以提高较高等级的传输安全保证。

FDL 层提供的服务有：

SDA（发送数据并要求回答）；

SDN（发送数据，不要求回答）；

SRD（发送数据并要求回送数据）；

CSRD（循环发送数据并要求回送数据）；

对于S7-300系统，要实现FDL通信，必须具有CP342-5、CP343-5通信处理器。由通信处理器完成FDL数据传输，每个通信处理器可同时与多个主站建立通信连接，连接个数与通信处理器型号有关。S7-200不支持FDL通信。

作者在2.2.3节中论述的STEP 7组态方法，也可用于判断通信处理器是否支持FDL通信，其原理在本质上是相同的，此处不再赘述。

2.2.5 PROFIBUS总线应用现状与展望

PROFIBUS总线的概念已成为一个在IEC61158和IEC61784中通用的开放标准。目前世界上大约130多万台PROFIBUS装置安装在流程工业现场。PROFIBUS现场总线技术在石油、化工、钢铁、汽车、水处理等行业产生着巨大效益。PROFIBUS国际组织（PI）主席Edgar Kuster先生表示：从各方面而言，PROFIBUS正在为流程工业和制造业做出贡献，这一成就使其它竞争技术相形见拙。同时，市场对PROFIBUS的热情有增无减。相信安装的PROFIBUS节点设备到2008年将再翻一番，达到两千万。可以相信，PROFIBUS总线凭借其出色的性能，将进入我国更多的行业领域，为企业带来更高的效益。因此，研究PROFIBUS通信技术有着重要的实际意义。

2.3 PROFInet通信技术研究

2.3.1 PROFInet技术特点[2]

PROFInet是PROFIBUS总线技术的纵向扩展，它是一个综合的自动化概念。在自动化技术趋向模块化、分布式、智能化时，这种概念已经显现为一种必然趋势。由于它的设计是一体化的，从工程设计到运行期（Runtime）以及对其它通信系统（如PROFIBUS 和OPC）的转换体系结构都使用统一的模型，PROFInet 满足了自动化技术的所有关键要求：

- 从现场层到使用Ethernet 的公司管理层的连续一致的通信；
- 用于整个自动化区域的与制造商无关的成套设备级的工程设计模型；
- 对其它系统的开放性；
- 实现IT 标准；
- 集成PROFIBUS总线段的能力，而不需要对它们进行任何改变。

PROFInet 规范将现有的 PROFIBUS 协议与 Microsoft 的自动化对象模型COM/DCOM标准、TCP/IP通信协议、以及工控软件互操作规范OPC技术等有机地结合成一体，实现一种向所有的自动化装置都是透明的、面向对象的和全新的结构体系。

PROFInet的基础是组件技术。在PROFInet中，每个设备都被看作一个具有组

件对象模型接口的自动化设备，同类设备都具有同样的 COM 接口。在系统中通过调用 COM 接口从而调用设备功能。组件模型使不同制造商遵循同一原则创建的组件之间能够混合应用，简化了通信编程。每一个智能设备中都有一个标准组件，智能设备的功能则通过对组件进行特定的编程完成。同类设备具有相同的内置组件，对外提供相同的 COM 接口，为不同厂家的设备之间提供了良好的互换性和互操作性。CBA（Component Based Automation，基于组件的自动化）即是随之提出的概念，西门子公司已经提供相关产品。

由于 DCOM 具有如下技术特点：每个程序模块无需存储各客户端，更无需下载程序本身，只要在服务器内存放一份 DCOM 部件，不同地方的用户即可通过网络访问这一 DCOM 部件，而且，使用 DCOM 部件构成的大型分布式程序，可以把处理相同工作的部分分割出来交给一个专门的软件模块完成，而其他程序或其他 DCOM 部件只需对其进行调用，即可获得所需信息，因此，PROFInet 构成从 I/O 层直至协调管理层的基于组件的分布式自动化系统的体系结构方案，PROFIBUS 技术可以在整个系统中无缝地集成。PROFIBUS 可以通过代理服务器（Proxy）很容易地实现与其他现场总线系统的集成。在该方案中，通过代理服务器将通用的 PROFIBUS 网络连接到工业以太网；通过以太网 TCP/IP 访问 PROFIBUS 设备是由 Proxy 使用远方程序调用和 Microsoft DCOM 进行处理的。代理服务器是一种实现自动化对象功能的软件模块，该自动化对象既代表了 PROFIBUS 用户，又代表了工业以太网上的其他 PROFInet 用户。

PROFInet 协议分为三类：PROFInet V1，响应时间在 10～100ms，它能满足大多数工厂应用；PROFInet V2，提供了一个优化的、基于软件的通信通道，通过这个通信通道，PFOFInet 可以获得等同、甚至超过传统现场总线的实时性能，响应时间在 5～10ms，能够满足传感器和执行器之间的数据交换；PROFInet V3，满足了对现场级设备进行运动控制对通信网络提出的苛刻的实时性要求，例如在包装机械和印刷机械中，其循环时间要小于 1ms。

2.3.2 PROFInet 通信模型

PROFInet 通信模型（见图 2.3.2.1）定义了一个与制造商无关的基于具有传统 IT 机制的 Ethernet 的通信标准，即运行期（Runtime）通信。它使用 PC 领域最通用的标准 TCP/IP 和 COM/DCOM，提供从办公领域到自动化层的直接存取（纵向集成），不同制造商的部件之间的数据可进行交换。在 Ethernet 上运行的设备需要实现符合 PROFInet 标准的通信机制。

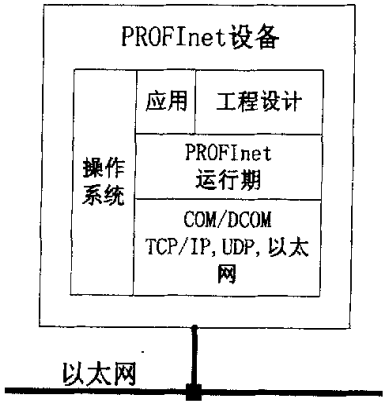


图 2.3.2.1 PROFInet 通信模型

为了满足自动化中的实时要求，PROFInet 规定了优化的实时通信通道：软件实时通道（SRT 通道）。这样一种解决方案极大地减少了通信栈上占用的时间，从而提高了自动化数据的刷新率方面的性能。一方面，几个协议层的去除减少了报文长度；另一方面，在需要传输的数据准备就绪发送以及应用准备就绪处理之前，只需要较少的时间。同时，大大地减少了设备通信所需要的处理器功能。PROFInet 中的实时通信通道如图 2.3.2.2 所示。

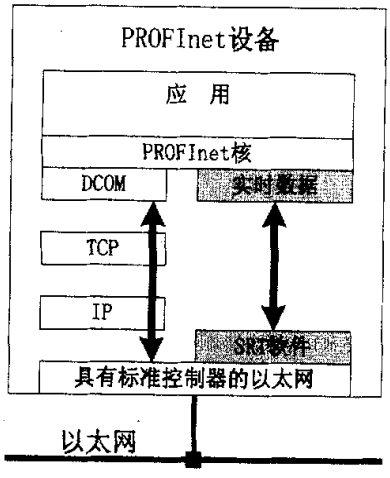


图 2.3.2.2 PROFInet 实时通信通道示意图

2.3.3 S7-200 与 S7-300 之间的 PROFInet 通信

作者研究了 S7-200 与 S7-300 之间的 PROFInet 通信，应用 PS 307 5A 电源（1 个）、CPU 314C-2DP（1 个）、CP343-1IT 以太网模块（1 个）、CPU 224（2 个）、CP243-1 以太网模块（2 个）、工业 ESM（电交换机，1 个）、编程计算机、PPI 电缆、MPI 电缆、普通以太网连接线等，设计了一个 PROFInet 通信网络，将两个 S7-200 客户端与一个 S7-300 服务器通过 ESM 连接，实现了数据交换。系统组成如图 2.3.3.1 所

示。

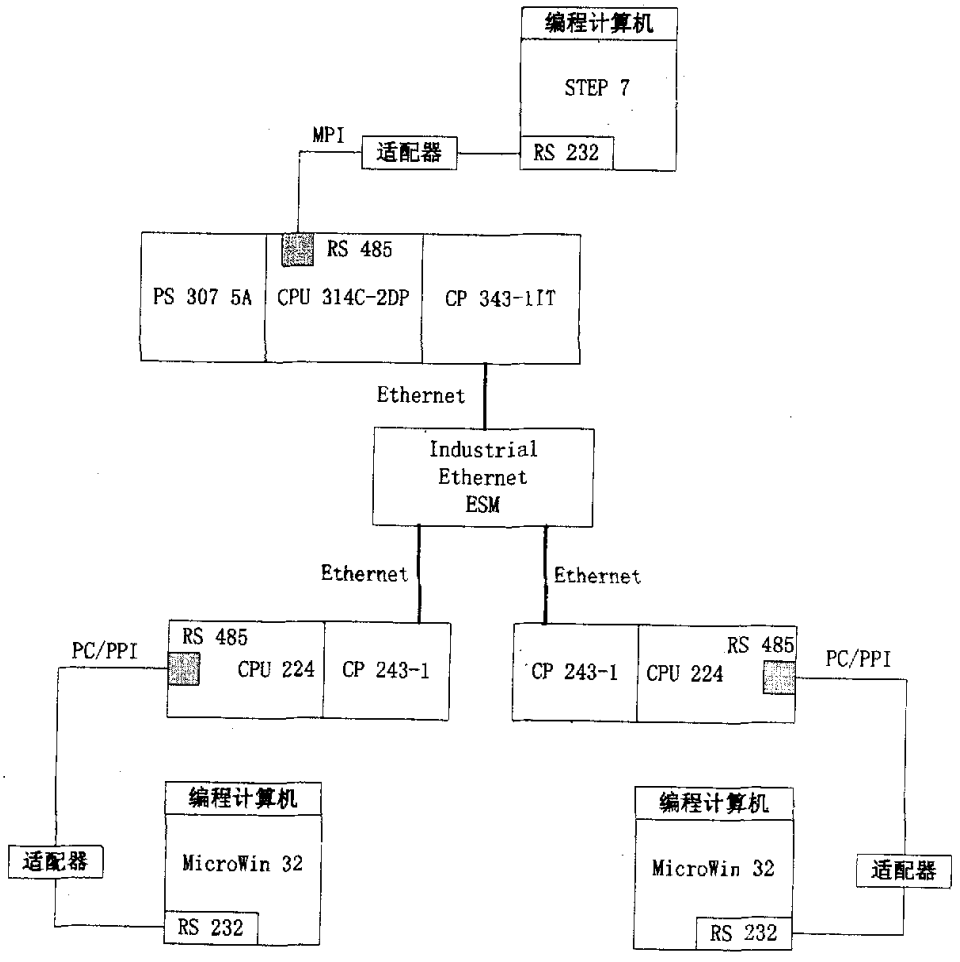


图 2.3.3.1 PROFInet 通信网络结构图

（1）S7-200 硬件组态与编程

STEP 7 MicroWin 32 V4.0 提供了以太网组态向导（Ethernet Wizard），方便用户配置以太网通信参数。此时需设置 CP243-1 以太网模块的 IP 地址、子网掩码、网关地址，如图 2.3.3.2 所示。这里分别将两个客户端的 IP 地址设为 192.168.1.2 和 192.168.1.3。

定义 S7-200 为客户端，指定服务器的 IP 地址（这里为 192.168.1.1），设置 TSAP 值（Transport Service Access Point，传输层服务访问点），如图 2.3.3.3 所示。对于 S7-200 客户端，TSAP 值从 10 开始，再加上连接号（这里为 0），因此它的 TSAP 为 10.00。对于 S7-300 服务器，TSAP 值也从 10 开始，加上机架号（这里为 0），再加上 CP343-1IT 模块所在插槽号（这里为 4，与 S7-300 的硬件组态有关），因此它的 TSAP 为 10.04。分配数据交换区（Data Transfers），如图 2.3.3.4

所示。

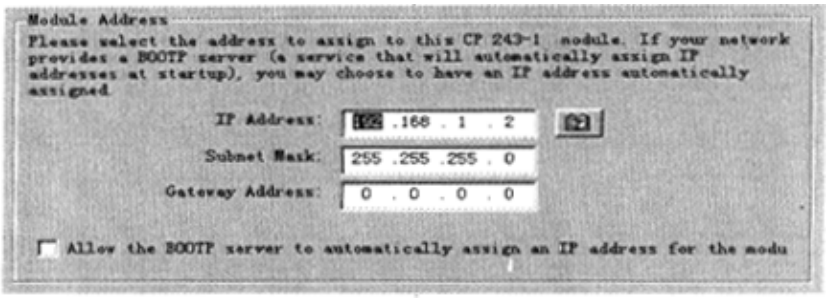


图 2.3.3.2 设置以太网模块的 IP 地址等

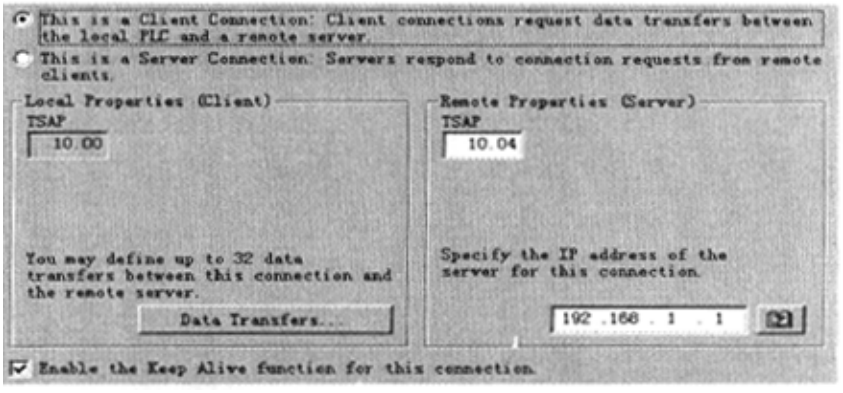


图 2.3.3.3 设置 TSAP 值与服务器 IP 地址

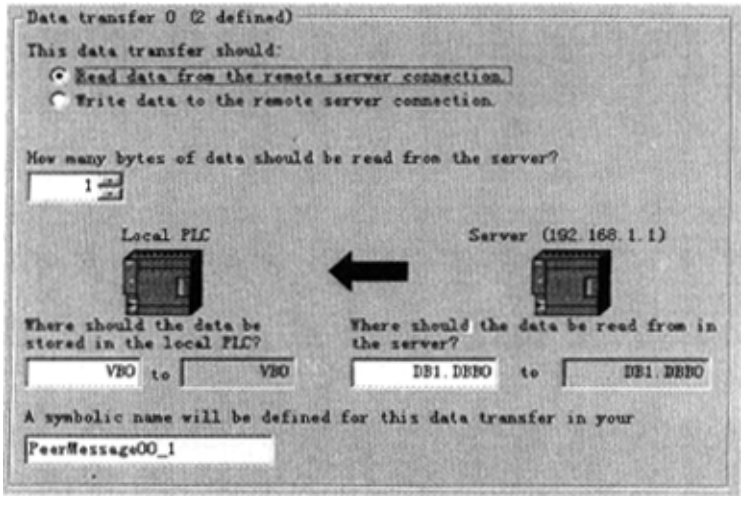


图 2.3.3.4 分配数据交换区

S7-200 组态完毕后，将自动生成以太网通信函数（ETH0_CTRL 和 ETH0_XFR）供用户调用。ETH0_CTRL 用于建立与服务器的以太网连接。ETH0_XFR 用于与服务器交换数据。

（2）S7-300 硬件组态与网络组态（NetPro）

硬件组态时（如图 2.3.3.5 所示），需为 CP343-1IT 以太网模块分配 IP 地址如 192.168.1.1，并指定交换机的 IP 地址（这里为 192.168.1.232），如图 2.3.3.6 所示。

图 2.3.3.5 S7-300 硬件组态

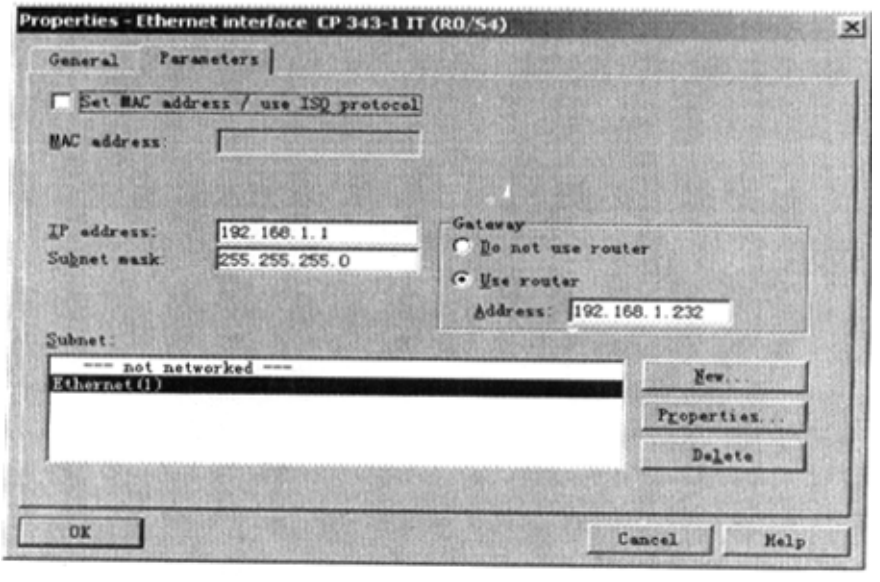


图 2.3.3.6 设置 CP343-1IT 的 IP 地址及交换机 IP 地址

硬件组态完成后，需进行网络组态，为服务器与两个客户端之间建立 S7 通信连接，并需设置 S7 连接的属性。由于是由 S7-200 激活服务器的以太网连接，因此需将“Establish an active connection”选项去掉，如图 2.3.3.7 所示。

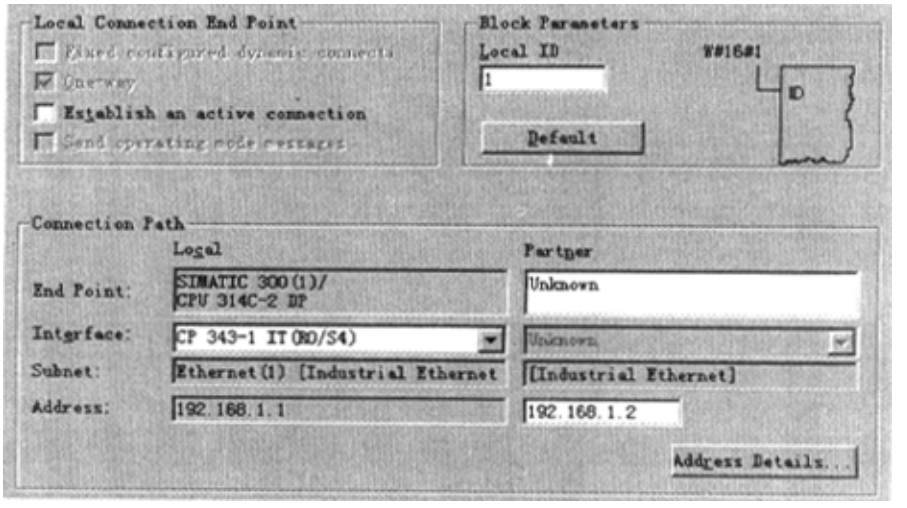


图 2.3.3.7 设置 S7 连接的属性

设置地址详细信息（Address Details），定义本地 TSAP 和远端 TSAP，如图 2.3.3.8 所示。远端 TSAP 即为 S7-200 中 Ethernet Wizard 配置时生成的客户端 TSAP（这里为 10.00）。本地 TSAP 则与 S7-200 中 Ethernet Wizard 配置时生成的 TSAP 值有所不同，因为二者的内容是有区别的：这里的 TSAP 从 10 开始，加上机架号（这里为 0），再加上 CPU 所在的插槽号（这里为 2），因此它的 TSAP 为 10.02。对于另一个客户端，它的 TSAP 则为 11.02，表示两个客户端各用一个以太网连接资源。

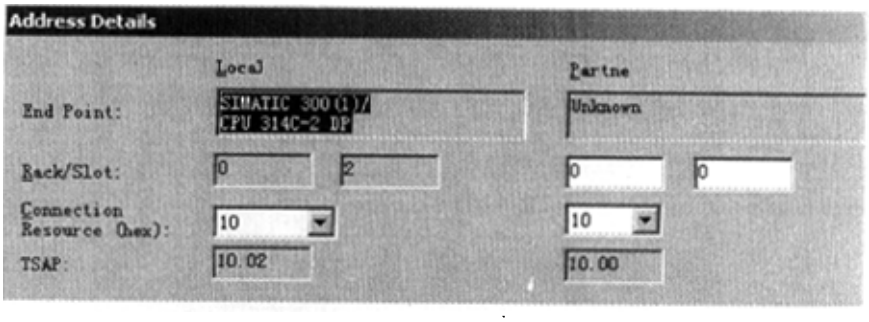


图 2.3.3.8 设置本地 TSAP 和远端 TSAP

至此，客户端和服务器的设置完毕，该 PROFInet 通信网络即可正常工作。若通过 TCP/IP 方式下载系统配置及程序数据，需将编程计算机的 IP 地址设置成与以太网模块的 IP 地址在同一网段内，否则无法通信。

2.3.4 PROFInet 应用前景探讨

PROFInet 正从企业级向现场级纵向渗透，这已成现实，并在工控界引起广泛讨论。目前它尚未得到大力推广，人们争论的问题主要是以下几个方面：

（1）通信确定性问题

由于以太网的 MAC 层协议是 CSMA/CD，在网络负荷较高时，以太网上存在的冲突成了主要问题，它极大地影响了数据吞吐量，造成了传输延迟，导致以太网实际性能下降。由于在连续 16 次冲突之后，报文会丢失，因此，节点之间的通信将无法得到保障，即存在通信不确定性问题。

针对这个问题，PROFInet 给出了相应的解决方案。对于运动控制这一对通信要求严格的领域，PROFInet 采用了 IRT（同步实时）的 ASIC 芯片。所谓同步实时，即反应时间极短，特别适用于快速的时钟同步运动控制应用的要求。

（2）工业可靠性问题

由于传统的以太网并不是为工业应用而设计的，没有考虑工业现场环境的适应性需要。工业现场的机械、气候、尘埃等恶劣条件对设备的工业可靠性提出更高的要求。因此，在工厂环境中，工业以太网必须具备良好的可靠性、可恢复性和可维护性。

PROFInet 则为以太网补充了以下重要性能，以解决工业可靠性问题：

- 冗余 24VDC 供电；
- 高速冗余的安全网络，最大网络重构时间为 0.3 秒；
- 用于严酷环境的网络元件，通过 EMC 测试；
- 简单高效的信号装置不断地监视网络元件；
- 使用 VB/VC 或组态软件即可监控管理网络。

（3）安全性问题

工业以太网将企业级、车间级、现场级合成一体，并与 Internet 无缝集成，实现数据共享，提高了工厂的运作效率，但同时也引入了一系列的网络安全问题，工业网络可能会受到病毒感染、黑客非法入侵与非法操作等网络安全的威胁。

PROFInet 中可采用网关或防火墙等将工业网络与外部网络进行隔离，还可以通过权限控制、数据加密等多种安全机制加强网络管理。

（4）现场总线集成问题

市场对 PROFInet 的认可取决于现有的现场总线安装设备能否容易地通过 PROFInet 扩展，从而保护用户早期的投资。PROFInet 提供了两种形式集成现场总线系统（如 PROFIBUS）：一是，通过代理服务器进行现场总线设备的集成，每台现场设备代表一个独立的 PROFInet 组件；二是，现场总线应用的集成，一个现场总线段代表一个独立的 PROFInet 组件，该组件包含 PROFInet 接口连接，因此，现场总线上设备和应用的全部功能可集成到以太网上。由于 PROFInet 定义了从现场总线向以太网转换的全透明策略，在基于 PROFInet 的系统中可继续使用 PROFIBUS 产品。

综上所述，PROFInet 是一个面向自动化未来的以太网现场总线解决方案，相信

将会越来越为人们所重视。

2.4 小结

MPI 通信适用于小范围的现场级通信，有三种通信方式：全局数据包通信方式、无组态连接通信方式、组态连接通信方式。全局数据包通信方式需要预先组态，适用于 S7-300、S7-400 系列 PLC 之间的通信。该通信方式无需编写通信程序，应用较为方便，但受 CPU 所支持的通信区大小的限制，如 S7-300 CPU 支持最大 22 字节地址区。无组态连接通信方式分单边编程通信方式与双边编程通信方式。单边编程通信方式只需在一方 PLC 编程，访问另一方 PLC，适用于 S7-200、S7-300、S7-400 PLC 之间的通信。双边编程通信方式需要对双方 PLC 调用系统功能块，适用于 S7-300、S7-400 PLC 的通信。组态连接通信方式仅适合 S7-300 与 S7-400 或者 S7-400 之间的通信，该方式下的每个数据包发送和接收的数据量比全局数据包方式和无组态连接方式的数据量大，但需进行网络组态建立连接表，占用 CPU 通信资源，因此，在满足通信要求时，可优先选择全局数据包方式和无组态连接方式。

PROFIBUS 是目前国际上通用的现场总线标准之一，它信息集成能力强，开放性、互操作性好，系统结构简单、可扩展性好，可靠性与可维护性高，因此得到众多厂商的支持，在现场总线领域遥遥领先。基于 PROFIBUS-DP 的 DX 通信方式给从站间交换数据提供了途径，无需在主站中编写通信程序。DX 通信方式是基于主/从站间的 MS 模式的，因此，在组态 DX 通信方式之前需要先组态从站与主站之间的 MS 通信，而且一般说来，遵循先组态从站，再组态主站的组态顺序。在 2.2.3 节中总结了 DX 通信实现的硬件条件，并给出了应用 STEP 7 软件判断 CPU 是否支持 DX 通信的详细方法。基于 PROFIBUS-DP 的 FDL 通信方式是进行在 PROFIBUS 参考模型中的第二层数据链路层上的通信。由于数据链路层本身的功能特点，使 FDL 通信具有较高等级的传输安全保证。只有 PROFIBUS 通信处理器支持 FDL 通信，至于何种型号的通信处理器支持 FDL 通信，仍可通过 STEP 7 软件进行判断。

PROFInet 是 PROFIBUS 总线技术的纵向扩展。它以 Ethernet 为基础，将 SIMATIC NET 无缝集成到多媒体领域。PROFInet 提供了两种形式集成现场总线系统，并将现有的设备或现场总线段视为 PROFInet 上的组件，这有效保护了先期投资，并极大地延伸了数据共享的范围，增强了自动化系统的功能。尽管人们对其实时性、可靠性、安全性提出质疑，但随着技术的不断进步，PROFInet 将会逐步完善，并逐渐被人们所接受。

西门子工业控制网络中的通信技术内容丰富，本章选取了上述最常见常用的通信技术进行了研究，还有其它如 ESM 对 PROFInet 通信网络的冗余管理技术、PROFInet 与 Internet 的集成技术、无线通信技术、串行通信技术、AS-i 通信技术等有待进一步研究和学习。

3 OPC接口技术研究

第2章讨论的SIMATIC NET中的通信技术为控制设备间的数据传递提供了各种有效途径，而本章中研究的OPC（OLE for Process Control）接口技术则提供了一个应用程序之间的标准接口，将这些控制设备的原始数据向上层传递，供HMI或上位机应用程序（如历史数据库应用程序）使用。

3.1 OPC提出的背景

随着工业自动化系统功能不断增强，工业现场中产自不同厂家的软硬件之间的数据交换成为突出的矛盾。虽然在不同系统之间可以采用DDE（直接数据交换）、WINSOCK等技术进行通信，但这些方法并非针对工业系统而设计，在实际应用中存在工作量大、系统稳定性差等缺点。另外各个厂家的软件对控制系统硬件操作的设备驱动程序接口也各不相同。为了对市场上不同厂家的设备统一管理，控制软件厂家必须针对市场上的各种常用设备开发设备驱动程序，而且当硬件设备升级、修改时，驱动程序也必须作相应修改，这种代价极高。如果设备驱动程序由硬件设备制造厂开发，那么它们也必须为市场上所有的工业控制软件开发驱动程序，代价同样非常高。

因此，有必要为工业控制系统应用程序的通信建立一个接口标准，即OPC接口标准，在工业控制设备与控制软件之间建立统一的数据存取规范。这个接口规范不仅能够应用于单台计算机，而且可以支持网络上分布式应用程序之间的通信，以及不同平台上应用程序之间的通信[31][33]。

3.2 OPC技术规范

管理OPC标准的组织是OPC基金会，其前身由一个Fisher-Rosemount、Rockwell Software、SIEMENS、Opto22、Intellution和Intuitive Technology等著名大公司组成专门的工作组，仅仅用了短短的一年时间便开发出一个基本可运行的OPC技术规范。

OPC以微软的OLE（现在成为ActiveX）、COM（组件对象模型）和DCOM（分布式组件对象模型）技术为基础，包括一整套接口、属性和方法的标准集，用于过程控制和制造业自动化系统。它采用客户机/服务器模式，由硬件生产商或第三方厂商根据数据访问接口标准开发硬件访问接口[34][35]。

ActiveX/COM技术定义了各种不同的软件部件如何交互使用和分享数据。不论过程中采用什么软件或设备，OPC为多种多样的过程控制设备之间的通信提供了公用的接口。依据接口标准，用户就可以访问到所需要的现场数据，而不必关心该数据从某个具体的硬件获取的技术细节。

OPC技术规范定义了OPC服务器提供给其它应用程序的两种接口：通用接口和

定制接口，如图3.2.1所示。

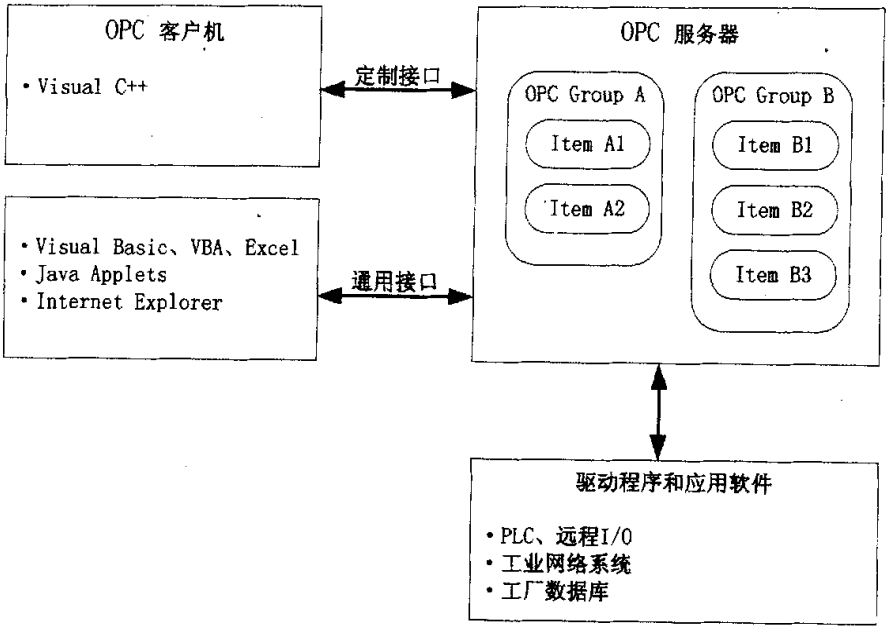


图3.2.1 OPC接口示意图

定制接口是OPC服务器所必须实现的接口，它描述了OPC组件对象的接口和方法，适合于用C++和PASCAL语言设计，并可实现最佳运行性能的客户应用程序。通用接口是可选的接口，它提供了一个自动配置和存取过程控制数据的接口,它方便了Visual Basic、Excel及其它可使用OLE自动化服务器应用程序接口的高级商业软件的使用。

（1）OPC数据访问规范

OPC数据访问规范（OPC Data Access）简化了不同总线标准之间的数据访问机制，为不同总线标准提供了通过标准接口访问现场数据的基本方法。OPC/DA服务器通过一个主设备（PROFIBUS总线上的一类主站）与一个总线网段相连，并通过该主设备访问网段上的其它设备，将访问到的数据用统一的OPC/DA接口形式进行组织，从而可被任一具有OPC/DA访问接口的应用程序访问。OPC/DA服务器屏蔽了不同总线通信协议之间的差异，为上层应用程序提供统一的访问接口，便于在应用层实现对来自不同总线协议的设备进行互操作。

OPC/DA服务器包括三类对象：服务器（Server）、组（Group）和数据项（Item）。OPC服务器对象维护有关服务器的信息并作为OPC组对象的容器。OPC组提供了客户程序组织数据的手段。OPC组对象维护有关其自身的信息，提供包含OPC项的机制，并管理OPC项。组有两种类型：公共组和局部组。公共组可以被多个客户共享，而局部组只能被一个客户使用。每个组中都可以定义一个或多个数据项。OPC组有

以下主要属性：

Name---组的名字；

Active---组的激活状态标志；

UpdateRate---OPC 服务器向客户程序提交的数据的刷新速率；

PercentDeadBand---数据死区（能引起数据变化的最小数值百分比）。

OPC 数据项代表与服务器中的数据的连接。使用 OPC 定制接口进行数据访问时，所有对 OPC 数据项的操作都是通过包容此数据项的 OPC 组对象进行的。每个数据项有以下几个属性：

. Active ---数据项的激活状态；

Value ---数据项的数值，为 Variant 类型；

Quality---数据项的品质，代表数值的可信度，为 Short 类型；

TimeStamp---时间戳，代表数据的存取时间。

OPC/DA 规范提供了统一的数据访问接口标准，但目前的 OPC/DA 规范尚有不足之处，因此仍在不断完善之中。由于 OPC 数据项的数据类型是 Variant 类型，该类型只可存放简单类型的数据，如整数和浮点数等，而不能存放结构体类型的数据。为了能访问总线设备中大量结构体类型的数据，OPC 基金会正着手制定新的规范 OPC/XML-DA。XML（eXtensible Markup Language，可扩展标记语言）可以描述结构类型数据，便于跨平台的数据交换。

OPC/DA 规范主要用于纵向的数据访问，即数据访问需要经历从应用程序到 OPC/DA 服务器再到总线设备的过程。当总线设备间进行横向的数据访问时，则需要依据下面的 OPC 数据交换规范。

（2）OPC 数据交换规范

OPC 数据交换规范 OPC/DX（OPC Data eXchange）给连接在以太网上的不同现场总线设备之间提供数据访问服务，同时也弥补了 OPC/DA 规范在实现总线设备间数据访问时对上层应用程序有依赖性的不足。

OPC/DX 通过 TCP/IP 协议为不同的以太网设备提供了服务器之间的横向数据访问，使服务器可以直接访问其他服务器的数据，而无需依赖于应用程序。因此，OPC/DX 规范可在现场设备层完成不同总线协议之间的互操作。OPC/DX 服务器的结构如图 3.2.2 所示。用户通过上位机组态软件可以配置总线设备之间的数据交换。OPC/DX 服务器同时也实现了 OPC/DA 服务器的功能，通过 OPC/DA 接口为其它 OPC/DA 客户端（包括上层应用程序和其它 OPC/DX 服务器）提供数据访问服务。OPC/DX 可作为 OPC/DA 客户端直接访问其它 OPC/DA 服务器（包括独立的 OPC/DA 服务器和 OPC/DX 服务器内部提供的 OPC/DA 服务器）。

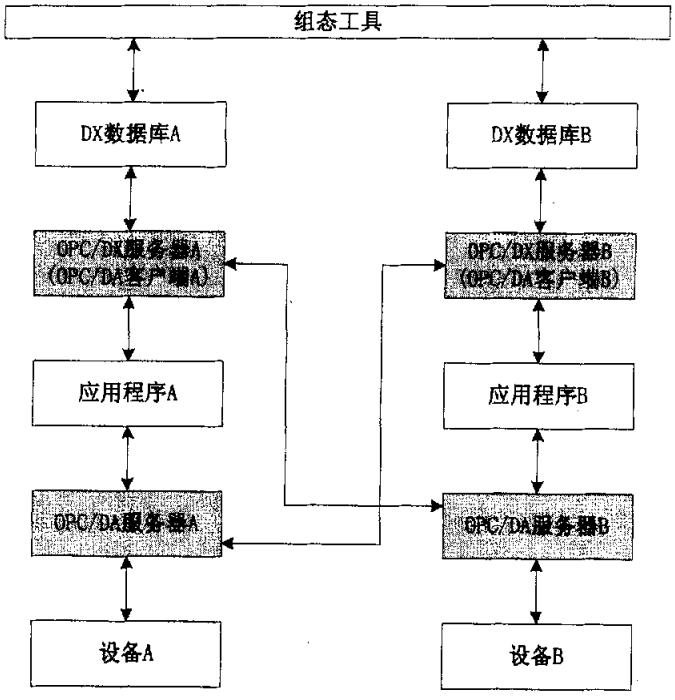


图 3.2.2 OPC/DX 服务器结构

（3）OPC 报警与事件规范

OPC 报警与事件（Alarm and Event）接口规范提供了一种机制。当 I/O 设备中有指定的事件或报警发生时，可通过这种机制通知 OPC 客户程序。

（4）OPC 历史数据存取规范

OPC 历史数据（Historical Data Access）存取规范支持下列两种历史数据服务器，向应用程序提供关于原始数据的所有信息。一是简单趋势数据服务器，提供原始数据和简单存储功能，数据以 OPC/DA 服务器提供的数据类型存储。二是复合数据压缩和分析服务器，提供数据压缩功能、数据汇总、数据分析（如求最大/最小值、平均值）等功能，还可保存对历史数据的注释信息。

（5）OPC 批处理过程规范

为批处理工业设计开发的产品不断增多，这些产品间的以及这些产品与其他系统间的数据交换的需求也不断增多，如管理设备（测控站、控制站等）、过程控制系统（实验室系统、批控制系统、称重系统等）和企业管理系统（ERP、MES 等）。通常大多数批处理系统使用自己的接口分发和收集数据，这样就无法用即插即用的方式扩展现有的系统。采用互相开放的解决方案即 OPC 批处理过程规范对解决这一问题具有非常重要的意义。

批处理数据交换规定了四个基本信息类型：设备容量、当前的操作情况、历史

数据和批处理内容。

（6）OPC 保密性规范

OPC 保密性（Security）规范定义了 OPC 服务器的三个安全等级，对服务器中指定的资源进行保护：一是无保密性，即 OPC 服务器不对客户端的访问作验证；二是 DCOM 保密性，该保密等级在 Windows NT 操作系统下有效，由 DCOM 安全机制限制客户端访问权限，而 OPC 服务器本身并不验证客户端的合法性；三是 OPC 保密性，该保密等级才是真正意义上由 OPC 服务器自身控制内部对象的访问权限。OPC 保密性规范有效管理和加强了系统信息的安全性。

3.3 OPC 接口技术在 SIMATIC NET 中的应用分析

由于 OPC 接口技术具有开放性（Openness）、高生产率（Productivity）、“即插即用”的可连接性（Connectivity），它在 SIMATIC NET 控制网络中也得到了广泛的应用，如用于在线数据监测、报警和事件处理、历史数据访问、远程数据访问等。

3.3.1 OPC 在 S7-200 系统中的应用

对于 S7-200 系统，西门子公司新推出了 PC Access V1.0，用于支持 OPC 方式的通信，提供了 OPC/DA 2.05 版本的 OPC 服务器：S7200.OPCServer。它支持的数据存取途径包括：PPI（通过 RS232 PPI 电缆或 USB PPI 电缆连接）、MPI/PROFIBUS（通过西门子公司提供的通信板卡）、以太网（通过通信模块 CP243-1 或 CP243-1IT）、内置或外置的 Modem（调制解调器）以及 Modem 通信扩展模块 EM 241。

通过 PC Access 可对单个或多个 S7-200 PLC 站的变量进行操作。此时需要创建所要操作的数据项（如 NewItem），并设定数据项地址、数据类型（支持的数据类型见表 3.3.1.1）、读/写权限等，如图 3.3.1.1 所示。

表 3.3.1.1 PC Access 支持的数据类型

数据类型	位数	取值范围
BYTE	8	0～255
INT	16	-32768～32767
WORD	16	0～65535
DINT	32	-2147483648～2147483647
DWORD	32	0～4294967295
REAL	32	-3.402823e+38～3.402823e+38
BOOL	---	True (1), False (0)
STRING	---	1～254 字节

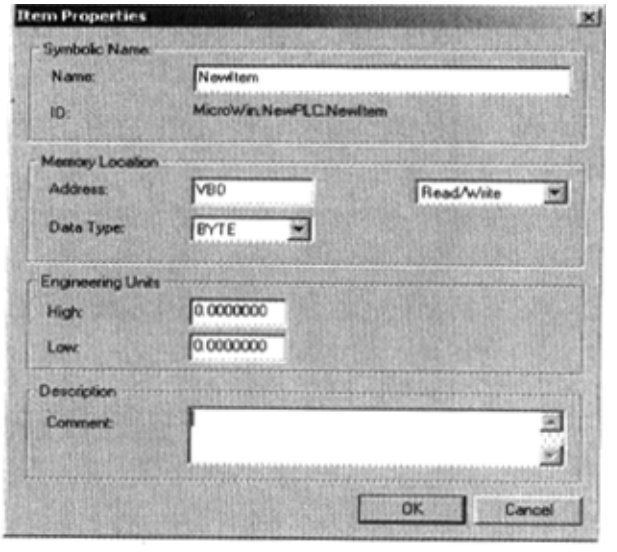


图 3.3.1.1 在 PC Access 中创建变量

然而这仅仅是 PC Access 软件的最基本的应用，更多的则是应用 S7200.OPCServer 进行具有定制功能的数据访问，这样数据操作的自由度就更大，如与 Microsoft Excel 客户端和 Protool/Pro（西门子监控组态软件）客户端交换数据。

PC Access 软件提供了 Excel 客户端的 VBA 插件（VBA 是指 Visual Basic for Application，它是在 Office 中使用的宏语言，主要为了增强 Word、Excel 等软件的自动化能力），可使 Excel 客户端从 S7-200 PC Access 的 OPC 服务器中获得数据。

在 Excel 中访问 S7-200 PLC 数据之前，先要进行 Excel 客户端配置，即加载 VBA 插件。在 Excel 中加载宏“OPCS7200ExcelAddin.XLA”，它位于 S7-200 PC Access 的安装目录的 Bin 文件夹中。加载完毕后，Excel 中即新增了一项宏：OPC-Client AddIn for Excel，如图 3.3.1.2 所示。

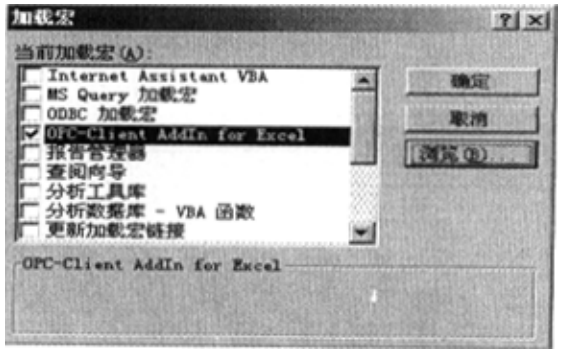


图 3.3.1.2 在 Excel 中加载 OPC 客户端的宏

由于该 VBA 提供了通过 OPC/DA 访问 S7200.OPCServer 的途径，因此，可以很方便地在 Excel 中读/写 S7-200 PLC 中的变量。

如读变量操作：

```
Dim str As String
str=Excel.Application.Run("OPCS7200ExcelAddin.XLA!OPCRead",2,VW100,
WORD,RW", "")
Cells(1, 1).Offset(0, 0) = str
```

该读操作方便的将站地址为 2 的 S7-200 站中的 VW100 读出并显示于 Excel 的“A1”单元。

写变量操作：

```
Excel.Application.Run("OPCS7200ExcelAddin.XLA!OPCWrite",2,VW100,WOR
D,RW",Cells(2, 2), "")
```

该写操作将“B2”单元中的数值赋给站地址为 2 的 S7-200 站的变量 VW100。

因此，通过该 Excel 的 VBA 插件，可以便捷地以报表、图表的形式显示 S7-200 站中的变量，并直接存储为 Excel 文档。

此外，S7-200 PC Access 还支持 SIMATIC Protool/Pro（监控组态软件）客户端，为 S7-200 系统的监控提供了又一条重要途径。

对于将在 Protool 中监控的变量（如 NewItem_VW0 和 NewItem_VW2），需要先在 PC Access 中创建，设置访问权限等，并保存，目的是将变量加入 S7200.OPCServer。在 Protool/Pro CS（组态、设计环境）中需要设置 S7-200 控制器与 Protool 监控程序之间通信的驱动程序为“OPC V6.0”，如图 3.3.1.3 所示。

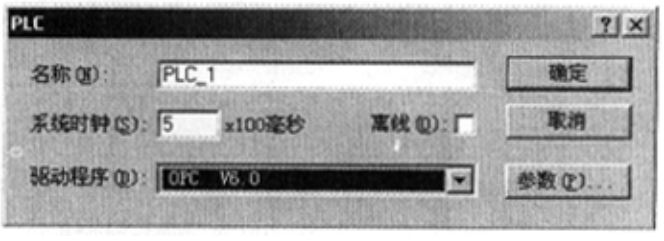


图 3.3.1.3 设置 OPC 驱动程序

在参数选择时，需选择服务器名称：“S7200.OPCServer”，如图 3.3.1.4 所示。此时可选择本地 OPC 服务器（Local Server），也可用位于网络上的 OPC 服务器（Network Neighborhood）。若选用位于网络上的 OPC 服务器，则需对服务器和客户端的 DCOM 属性进行相关配置，方可进行正常通信，配置方法将在 3.4 节中进行研究。

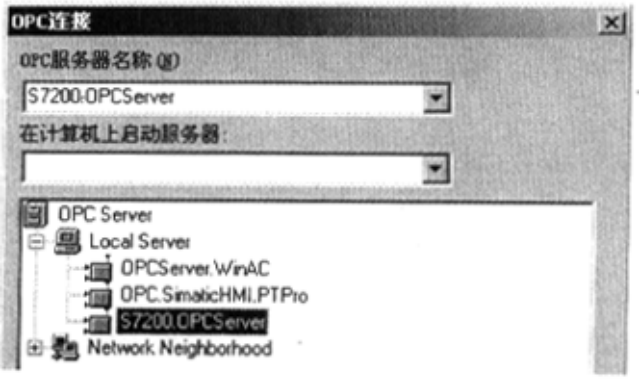


图 3.3.1.4 OPC 服务器选择

至此，Protool/Pro 客户端配置完毕。然后就可以在 Protool/Pro 中选择已加入服务器的变量（如图 3.3.1.5 所示），并进行监控。

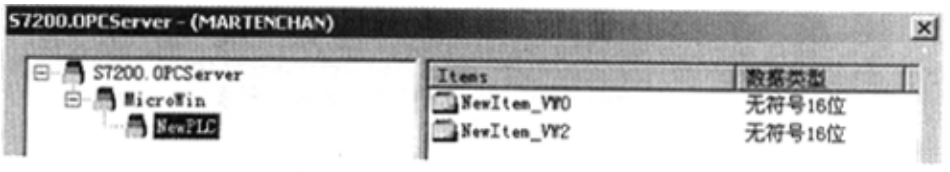


图 3.3.1.5 选择服务器中的变量

不妨编写 S7-200 程序实现 VW2 = VW0 + 1，且在 Protool 中定义文本输入域 VW0 和文本输出域 VW2，监控 PLC 中的变量。Protool 程序的运行结果如图 3.3.1.6 所示。

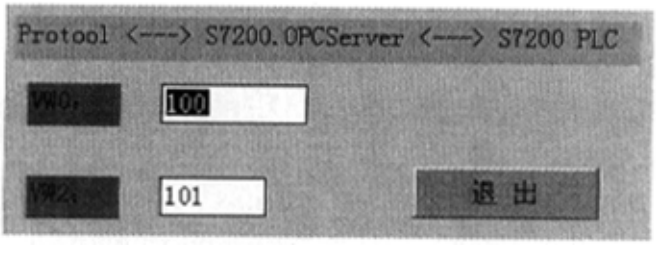


图 3.3.1.6 Protool 运行结果

可见，通过 OPC 方式，应用 Protool 对 S7-200 系统进行监控是可行的。

3.3.2 OPC 在 HMI 中的应用

注意到，在 3.3.1 节中讨论的 Protool 的运行系统是作为 OPC 客户机的，与之通信的是 S7-200 系统的服务器 S7200.OPCServer。

由于 Protool/Pro 软件也发布了供其它应用程序进行数据访问的 OPC 服务器：OPC.SimaticHMI.PTPro，因此也可以将 Protool 运行系统作为服务器使用。此时则需要组态 Protool 运行系统为服务器，供其它应用程序访问。用户应先组态 OPC 服务器，再组态 OPC 客户机，因为在组态 OPC 客户机时，已经在访问 OPC 服务器的数

据管理系统。此时需在 Protool 中设置系统为服务器，如图 3.3.2.1 所示。

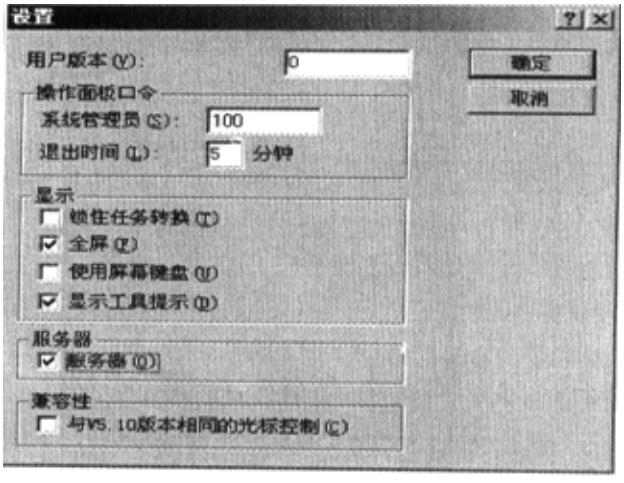


图 3.3.2.1 设置 Protool 运行系统为 OPC 服务器

此外，作为 SIEMENS HMI 中的另一重要成员：WinCC（Windows Control Center）组态软件也可通过 OPC 接口进行监控。它提供 OPC/DA 服务器 OPCServer.WinCC 和 OPC 报警/事件服务器 OPCServerAE.WinCC，供其它客户端访问，这里不作研究。

3.3.3 OPC 在 S7-300 系统中的应用

在 S7-300 系统中应用 OPC，需要 SIMATIC NET 软件的支持。SIMATIC NET 6.2 版本支持 DP、FDL、FMS、S7、ISO/TCP 等协议，通过 CPU 集成的 DP 口或以太网模块的 Ethernet 接口向服务器传递现场设备数据，供 HMI 或 SCADA（Supervisory Control and Data Acquisition，数据采集与监控系统）应用程序访问，其数据存取均按 3.2 节中讨论的 OPC 规范进行。

3.4 OPC 服务器/客户机配置

OPC 在本地（local）运行是其最基本的应用。由于 OPC 基于 DCOM 技术，因此，它也适用于远程访问。作者实现了局域网内对 S7-200 系统基于 OPC 方式的远程访问，系统连接如图 3.4.1 所示。

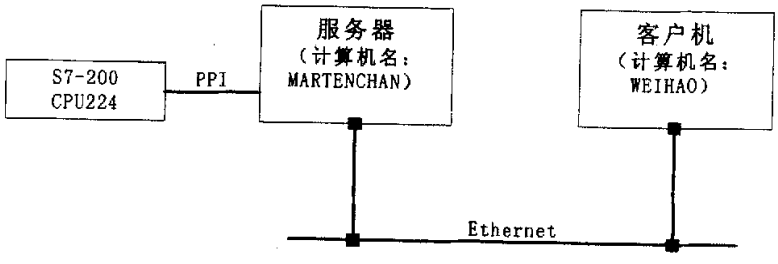


图 3.4.1 OPC 服务器/客户机方式访问 S7-200 PLC

此时在服务器端和客户端都需要安装 PC Access，并对 OPC 服务器与客户机的 DCOM 进行相应的配置。

服务器端配置如下：

（1）首先确保 Windows NT 的 GUEST 用户没有被禁用。

（2）在计算机服务器（MARTENCHAN）上运行 dcomcnfg 程序，进行 DCOM 配置。

（3）进入 DCOM 的总体默认属性页面，启用分布式 COM，并将默认身份级别改为“无”。

（4）进入 DCOM 的总体默认安全机制页面，确认默认访问权限和默认启动权限中的默认值无 EveryOne，如不去掉 EveryOne，应用服务器不能正常启动。

（5）在常规页面中，选择应用服务器：S7200 PC Access OPC Server，如图 3.4.2 所示，并继续设置其属性。

（6）将常规页面中的身份验证级别改为“无”。

（7）位置页面中选择“在这台计算机上运行应用程序”。

（8）将安全性页面设置中，均选择“使用自定义访问权限”，编辑每一个权限，将 EveryOne 加入用户列表中。

（9）身份标识页面中，选择“交互式用户”。

图 3.4.2 选择 S7-200 的 OPC 服务器

然后再设置客户机（WEIHAO）的 DCOM：

（1）启动 dcomcnfg 配置。

（2）常规页面中，打开应用服务器（S7200 PC Access OPC Server）的 DCOM 属性设置。

（3）将常规页面中的身份验证级别改为“无”。

（4）身份标识页面中，选择“交互式用户”。

（5）位置页面中设置中间层的机器，即服务器 MARTENCHAN，如图 3.4.3 所示。

（6）进入 DCOM 的总体默认属性页面，设置“在这台计算机上启用分布式 COM”，将默认身份级别改为“无”。

至此，服务器、客户端配置完毕。在客户机 WEIHAO 上运行 OPC 客户端程序，即可访问与服务器端相连的 S7-200 PLC 中的数据。OPC 客户端程序的开发方法将在 3.5 节中进行研究与探讨。

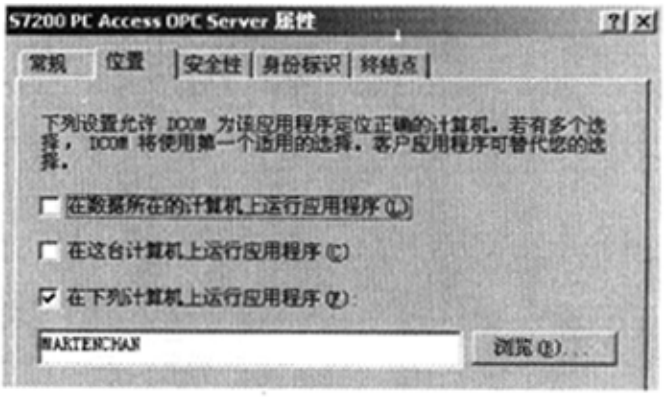


图 3.4.3 设置服务器端计算机

3.5 基于 OPC/DA 规范与 S7-200 系统的配方演示系统设计

在 3.3.2 节中讨论了用 Protool/Pro 监控 S7-200 的方法，然而对于某些小型项目或教学实验系统而言，也可自行开发基于 OPC/DA 规范的 OPC 客户端应用程序。本节以基于 S7-200 的配方演示系统为例，研究了应用 Visual Basic 6.0（VB 6.0）设计 OPC 客户端应用程序的方法。

3.5.1 配方系统简介

配方是与某一特定生产工艺过程相关的所有参数的集合，这一工艺过程的每一个参数叫做配方的一个条目，这些参数的每一组特定值，叫做配方的一条数据记录。使用配方的目的是能够集中并同步地将某一工艺过程相关的所有参数以数据记录的形式从操作单元传送到 PLC，或从 PLC 传送到操作单元。

本节设计的配方系统根据原料：水、果汁、香料的配比，及混合温度、搅拌速度、搅拌时间的不同，可生产出不同的饮料产品，如果汁饮料、浓缩果汁、纯果汁等。工艺流程图如 3.5.1.1～3.5.1.4 所示。

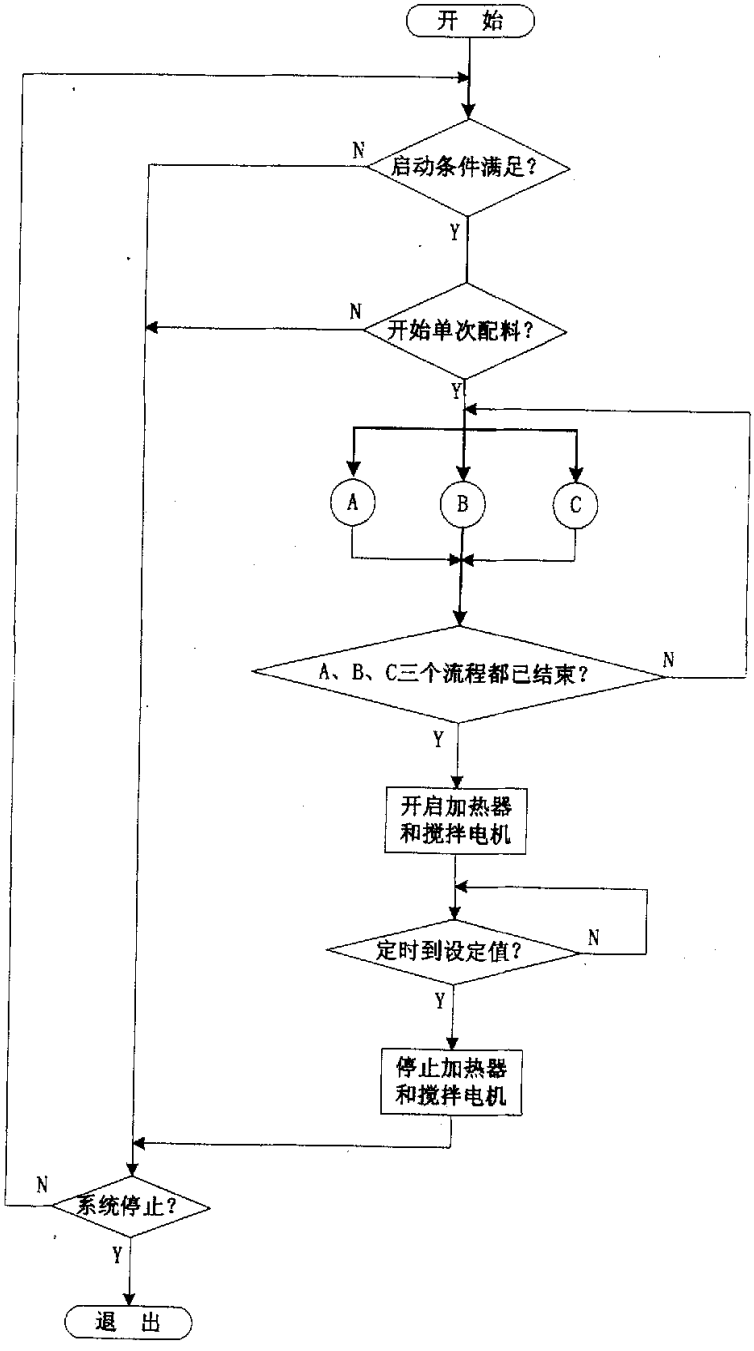


图 3.5.1.1 配方系统工艺流程图

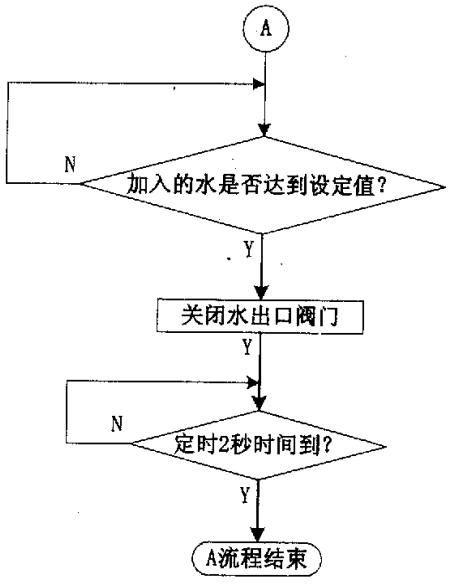


图 3.5.1.2 配方系统流程图 A

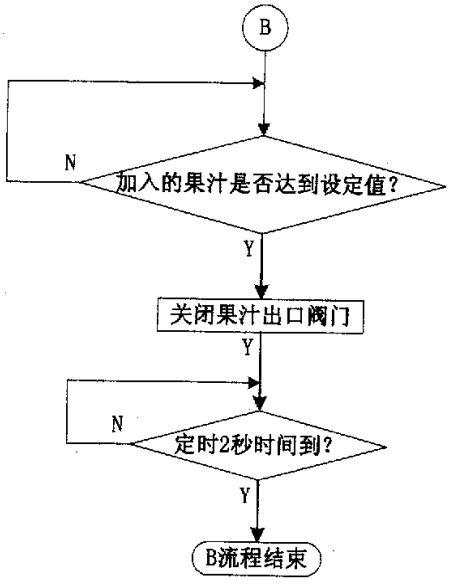


图 3.5.1.3 配方系统流程图 B

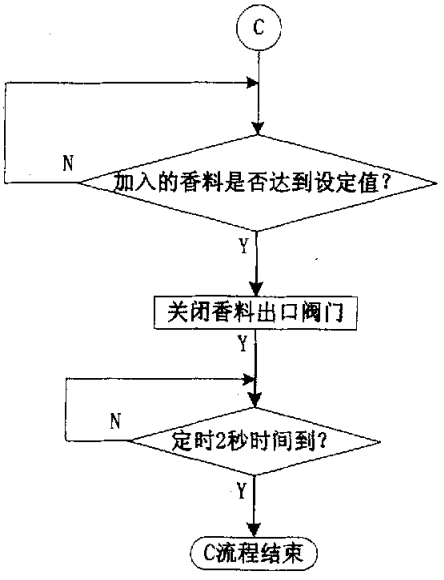


图 3.5.1.4 配方系统流程图 C

3.5.2 开发方案选择

对于开发基于 S7-200 的配方系统，西门子公司在 S7-200 编程环境 MicroWin32 V4.0 中提供了配方向导（Recipe Wizard），只要预先建好若干数据记录，随程序一并下载至 PLC，然后在 PLC 程序中就可通过配方专用子函数调用各数据记录，以改变工艺参数。但这种方法需要 PLC 硬件支持，支持配方向导的 CPU 有 CPU 224（2.0 版本）、CPU 224XP（2.0 版本）和 CPU 226（2.0 版本）。当需要对版本在 2.0 以下的 CPU 实现配方控制时，OPC 方式也不失为一种值得尝试的方法。通过自行开发的 OPC 监控程序，也可实现配方控制，并且可设计更多的功能。

开发 OPC 客户端应用程序可以有两种方法：

一是使用 Visual C++及其本身提供的 COM 库函数进行开发。这种方法比较灵活，但要求开发人员对 OPC 规范的细节和 COM 技术原理有比较深入的理解。显然，难度较大，不利于快速开发。

二是使用第三方的动态链接库或工具包进行开发。“Knight OPC Client Rapid Development Toolkit”是这类工具包中使用较为频繁的一种，可用于 OPC 客户端程序和服务器端程序的开发。另外，在 OPC 基金会网站也提供通用的 OPC 开发包“OPC Core Components 2.0 SDK 2.2”。这两种工具包提供了最基本的 OPC 函数，因此程序设计灵活性较大，同时工作量也较大。此外，西门子公司的 PC Access 提供了免费的“SIEMENS OPC DAAutomation 2.0”，这是专门用于西门子自动化系统的 OPC 客户端开发工具包，它封装了 OPC 的部分功能，因此，用它开发基于 S7-200 系统的配方系统比用前两种工具包更方便、效率更高。由于 OPC 得到了 Microsoft 的支

持，与其它编程环境相比，Microsoft Visual Basic 跟它结合得更好，因此，作者选择了 Visual Baisic 6.0 作为开发环境。

3.5.3 配方系统监控程序设计

本节设计的配方监控程序通过 OPC 方式，可向 S7-200 PLC 下载配方，并控制其运行、停止，实时监视各原料罐的液位、各流量计的值、各阀门的状态等。配方可保存在监控计算机上，且可以通过“配方管理”功能进行添加配方、删除配方等编辑操作，以满足实际生产的需要，例如增减产品、调整产品配方等。配方系统监控程序运行的主界面如图 3.5.3.1 所示。

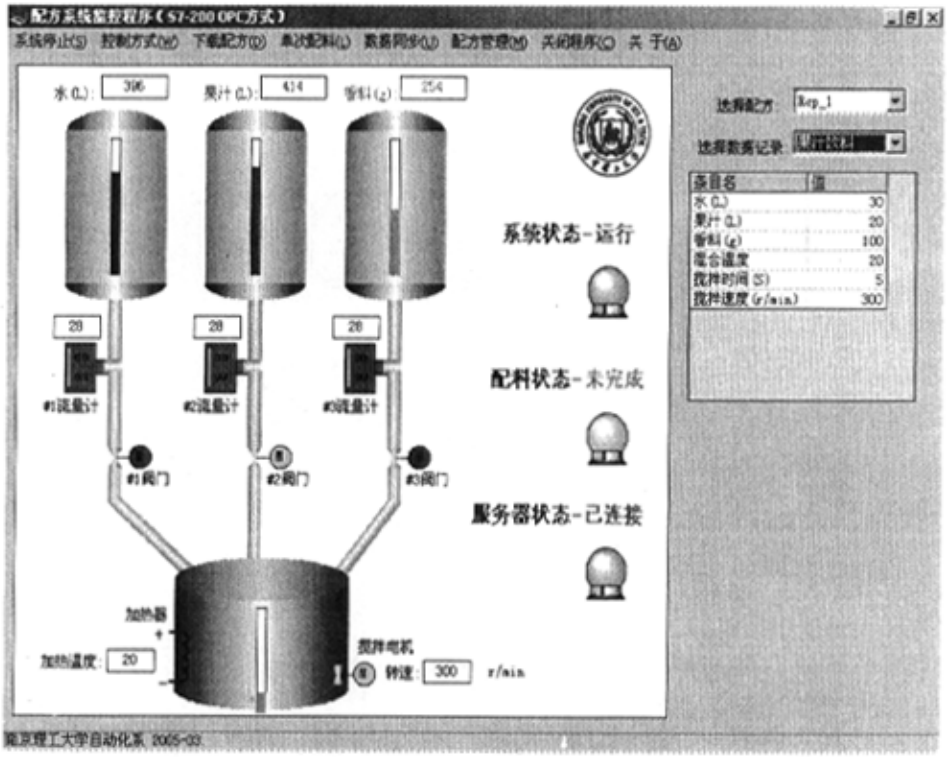


图 3.5.3.1 配方系统监控程序运行主界面

（1）OPC 通信初始化

为确保应用程序与 OPC 服务器之间正常通信，OPC 通信初始化需按照一定的流程进行，如图 3.5.3.2 所示。

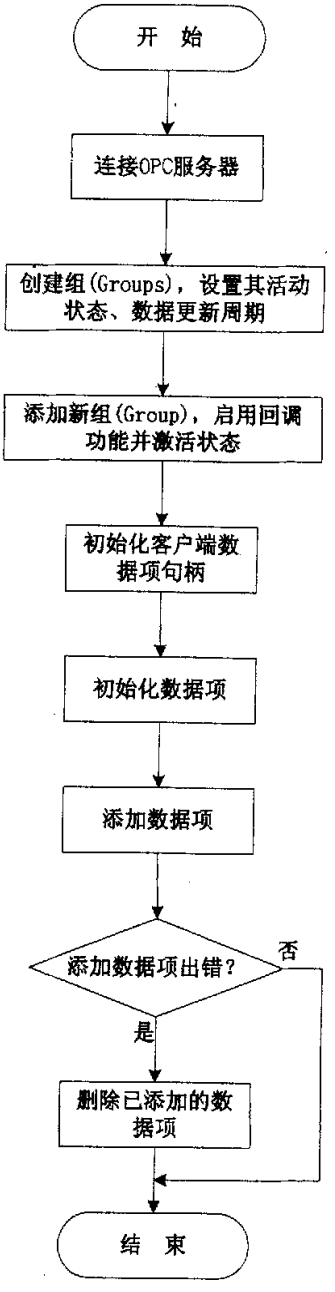


图 3.5.3.2 OPC通信初始化流程图

（2）接收数据

初始化完毕后，即可从服务器接受数据。注意，OPC组MyGroup的IsSubscribed属性必须为True，才能触发数据改变事件。当服务器上有数据发生变化时，触发DataChange事件，该事件的声明如下：

Private Sub MyGroup_DataChange(ByVal *TransactionID* As Long, ByVal

NumItems As Long, *ClientHandles()* As Long, *ItemValues()* As Variant, *Qualities()* As Long, *TimeStamps()* As Date)。

此时，根据客户端数据项的句柄以及返回的 Qualities（数据质量）进行过滤，可得到有效过程数据，并存储到 Variant 类型数组 MyValues() 中。作者构造了显示函数 DisplayValue(Values() As Variant)，将过程数据显示在界面上。DataChange 事件中的处理流程如图 3.5.3.3 所示。由于 DisplayValue 函数涉及的是图形处理知识，这里不展开介绍。

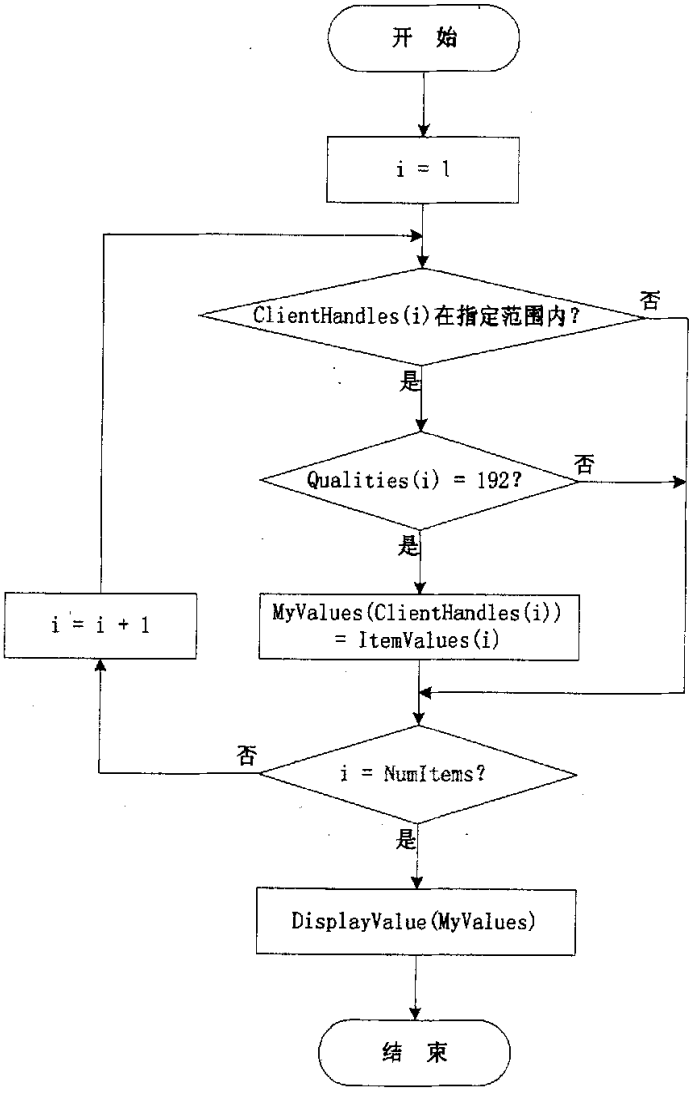


图 3.5.3.3 DataChange 事件处理流程图

（3）同步/异步读写数据

OPCGroup 提供了同步/异步读写数据的方法：SyncWrite（同步写）、AsyncWrite

（异步写）、SyncRead（同步读）、AsyncRead（异步读）。同步读写数据比较简单，而异步读写数据速度较慢，需与事件配合使用。方便起见，此处使用 OPCGroup 的同步读写数据方法或数据项 OPCItem 的 Read/Write 方法即能满足要求。对于需要整体读/写变量的场合，使用 OPCGroup 提供的读/写方法较为方便，而只需操作单个变量时，用 OPCItem 提供的读/写方法则较为恰当。

（4）配方管理模块设计

配方管理模块可管理以随机文件形式保存在磁盘上的配方文件（*.rcp），提供了新建配方、删除配方、新建数据记录、删除数据记录、修改数据记录等功能。每个配方中有若干个数据记录，因此为了方便操作各数据记录，在 VB 中定义了一个模块（Module）描述数据记录的结构：

```
Type Record
ID As Integer              '记录编号
strName As String * 20     '记录名称
Shui As Integer            '水
GuoZhi As Integer          '果汁
XiangLiao As Integer       '香料
HunHeWenDu As Integer      '混合温度
JiaoBanSuDu As Integer     '搅拌速度
JiaoBanShiJian As Integer  '搅拌时间
End Type
```

实现配方管理功能要用到的文件操作函数有：

Dir（*pathname*, *attributes*）：返回一个字符串，用以表示一个文件名、目录名或文件夹名称 *pathname*，它必须与指定的 *attributes* 模式或文件属性、或磁盘卷标相匹配。

Open *pathname* For *mode* As #*filenumber* Len = *reclength*：以 *mode* 模式打开文件（*pathname*），并指定文件号为 *filenumber*。对于随机文件，打开模式为 Random。对于用随机访问方式打开的文件，该值就是记录长度，即上述 *Record* 记录类型的长度。

Len（*varname*）：返回存储一变量所需的字节数。

LOF（*filenumber*）：返回用 Open 语句打开的文件的大小，该大小以字节为单位。

Get # *filenumber*, *recnumber*, *varname*：将一个已打开的磁盘文件读入一个变量之中。

Put # *filenumber*, *recnumber*, *varname*：将一个变量的数据写入磁盘文件中。

Close #*filenumberlist*：关闭 Open 语句所打开的输入/输出文件。

Kill *pathname*：从磁盘中删除文件。

配方管理界面如图 3.5.3.4 所示。

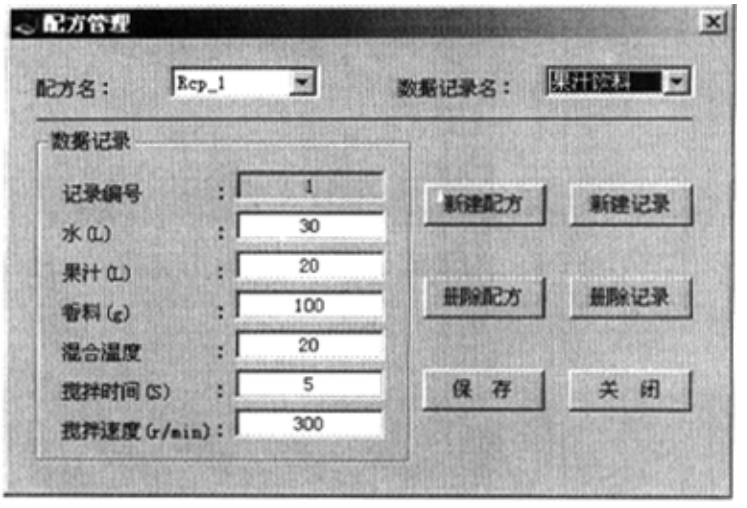


图 3.5.3.4 配方管理界面

（5）数据同步模块设计

当用户修改配方数据后，在监控界面中需更新最新数据，即“同步到本地”功能，此时只需从配方数据文件重新载入数据记录到监控程序。若要将最新数据记录下载到 PLC 中，则需调用“同步到 PLC”功能，此时将最新数据以同步方式写入初始化 OPC 通信流程时加入服务器的相应数据项中。

（6）程序退出模块设计

当退出程序时，需要对退出操作进行确认，以防误操作。

若确认退出监控程序，则需执行 OPC 通信初始化过程的逆过程，与 OPC 服务器断开连接，释放资源。流程图如 3.5.3.5 所示。

（7）出错处理

为增强程序的健壮性，需对与 OPC 操作、文件操作有关的过程、函数进行异常处理。异常处理程序结构一般如下：

```
On Error GoTo ErrorHandler
……              '(此处为受保护的代码)
Exit Sub
ErrorHandler:    '(异常处理代码，Err 对象中存放最近的错误信息)
   MsgBox Err.Description, vbCritical, "Error!"
```

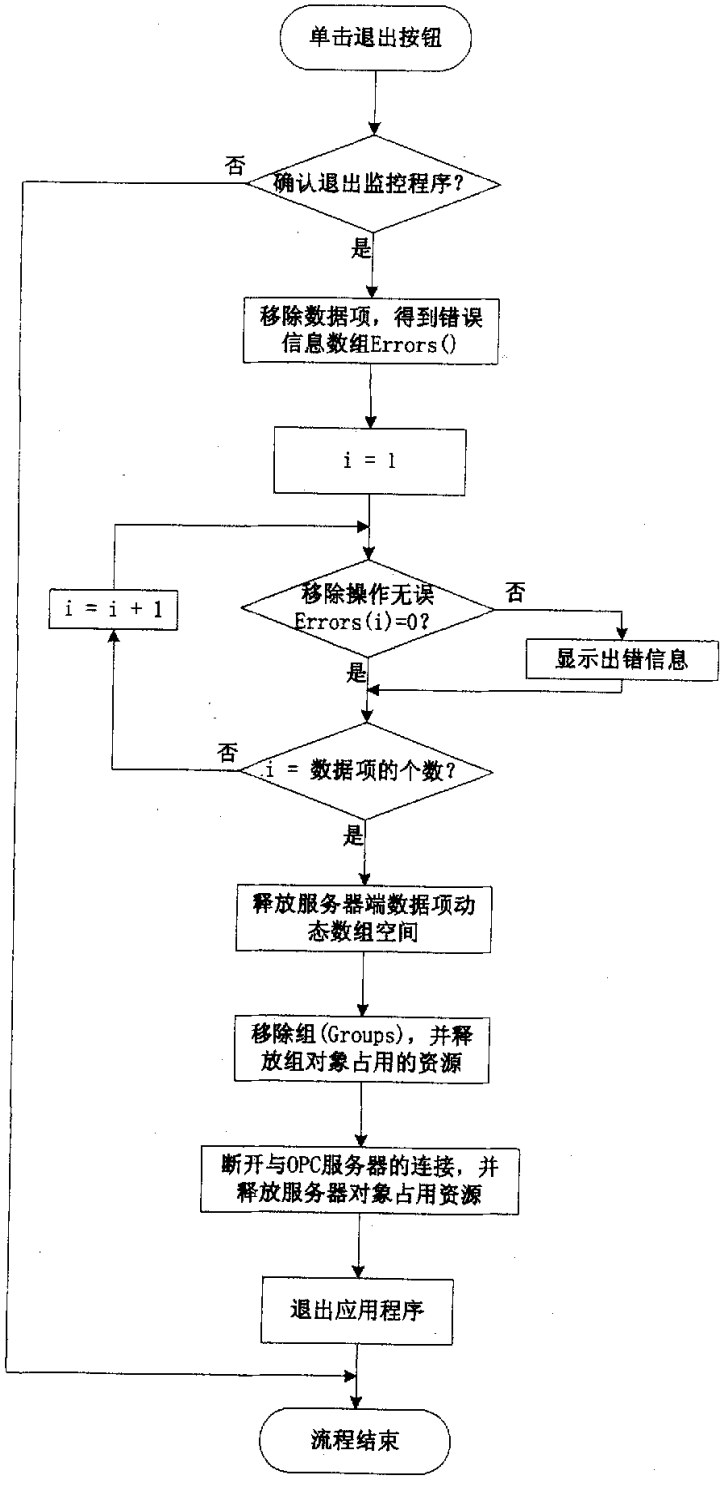


图 3.5.3.5 OPC 程序退出处理模块

3.5.4 PLC 控制程序设计

在 MicroWin 4.0 中设计 PLC 控制程序，为使程序具有良好的结构、较强的可读性和可维护性，可设计以下模块供主循环（MAIN）调用：

SBR_DI：系统的数字量输入信号（如启动信号）采集模块。

SBR_DO：系统的数字量输出信号（如阀门的开启/关闭信号）输出模块。

SBR_AI：系统的模拟量信号（如流量计）采集模块。

SBR_AO：系统的模拟量信号（如加热器控制电压）输出模块。

SBR_STOP：系统停止模块，对阀门、加热器、搅拌电机等执行机构的控制信号进行系统停止前的处理。

SBR_RUN：系统运行模块，执行配方系统的工艺流程。该配方系统的难点不在于控制程序的设计，因此对控制程序不作详细研究。

3.5.5 配方系统虚拟被控对象程序设计

该配方系统运行时，如果没有实际的外部输入，则可编写虚拟被控对象程序，用于演示该系统的运行过程，检验控制程序的正确性。设计思想：通过 OPC 方式，由上位机模拟实际被控对象的特性，并按一定周期读写 S7-200 PLC 中相应的变量。

在本例中，被控对象程序可模拟物料罐的液位传感器给 PLC 输入液位值，将其液位值通过 OPC 方式送给 S7-200 PLC。假设物料罐的液位仅跟开阀时间长短有关，假设其液位的变化率 $\Delta h=K*\Delta T$. 其中，比例系数 K 可调。可在被控对象程序界面上提供滑动条（Slider），调节 K 值的大小。这种虚拟被控对象方法在教学应用中具有一定的参考价值。被控对象程序的运行界面如图 3.5.5.1 所示。

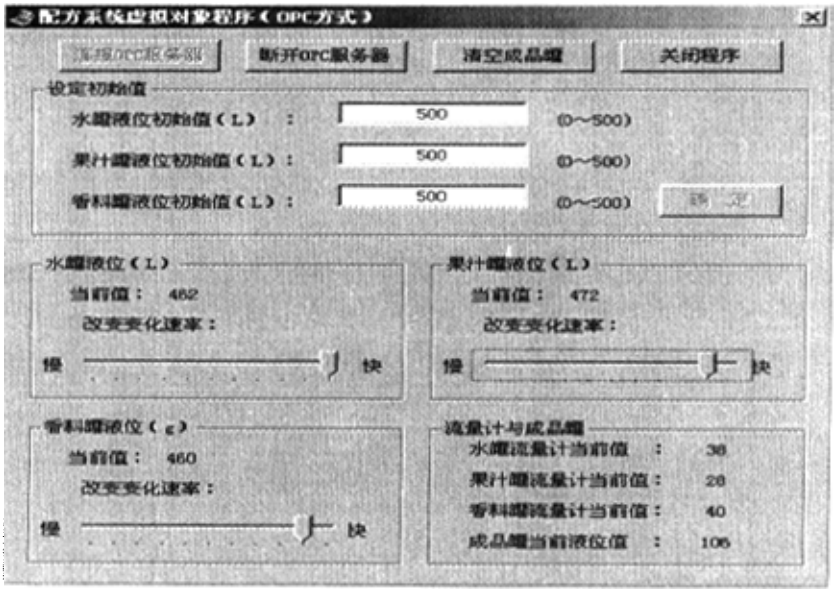


图 3.5.5.1 配方系统虚拟被控对象运行界面

由于被控对象程序也是通过OPC方式与S7-200 PLC通信，因此，设计方法与3.5.3节中研究的监控程序的OPC通信方法类似，不再赘述。

3.6 小结

OPC接口规范提供了连接数据提供源（OPC服务器）和数据的使用者（OPC应用程序）之间的软件接口标准，使用户以统一的方式去访问现场设备，这样数据提供者就不需要考虑应用程序的不同需求，同时数据的使用者也无需了解硬件的操作过程。OPC接口是具有高度柔软性的接口标准，它在S7-200、HMI、S7-300系统中已有很多应用。

此外，由于OPC接口的高度灵活性，这给用户通过第三方程序访问现场级设备数据提供了重要途径。第三方的应用可归纳为以下三点：

第一，OPC接口可应用于监控，且具有如下优点：

（1）节约成本。S7-200监控方案之一，需要EM 277扩展模块和CP通信板卡等附加硬件及诸如WinCC之类的监控软件，工程造价高。而基于OPC通信方式的监控方案只需安装PC Access V1.0，无需额外的通信模块，可自行编写OPC监控客户端程序。当然，通过前文3.3.1节和3.3.2节中讨论的方法，应用Protool/Pro的OPC接口，也可监控S7-200系统，需购买Protool/Pro软件，这种方法的可靠性比自行编写的OPC监控程序的要高，但灵活性不及后者。

（2）透明度高。还有一种监控方法，即用PPI协议编写监控程序，由于PPI协议是SIEMENS公司未公开的协议，因此与OPC方式相比，PPI协议并没有如此透明。

（3）通信速率高。也可利用西门子ProDave软件提供的DLL（动态链接库）函数进行通信，但一般而言调用DLL函数的方式没有OPC方式的通信速率快。西门子正用OPC方式取代以前的ProDave方式，因此OPC方式将会占据比ProDave更重要的位置，ProDave将会逐渐退出上下位机通信接口的舞台。

第二，还可应用OPC接口技术设计模拟被控对象，验证控制程序和监控程序的正确性，便于项目调试以及教学演示。

第三，也可开发小型OPC应用程序，用于设置少量PLC参数，以较低成本实现与PLC的数据交换。

总之，OPC接口成为不同现场级设备之间交换数据的标准接口，在工业控制系统中的应用相当广泛。

4 PCBCS解决方案—SIMATIC WinAC系统

4.1 PCBCS系统概述

当今的自动化系统趋向于信息化和分布式智能化，并具有开放的标准。越来越多的自动化任务如开环、闭环控制、运动控制等都已加入到典型的 PC 任务的范围内，这与 PC 技术的发展紧密相关。PC 的开放性保证了统一的开发环境、通用的网络结构和标准的程序接口。采用基于 PC 的自动化控制系统（PCBCS）可轻松地集成第三方软硬件产品，增强系统的灵活性，并降低系统集成、项目开发及维护的费用。

目前基于 PC 的自动化控制系统主要应用于以下几种方式[38][39][40]：

（1）现场总线 ＋ 分布式 I/O ＋ HMI

这种方式节省了电缆和硬件投资，简化了控制器与 HMI 的通信接口，降低了工程费用，同时还能提高通信速度。且可应用第 3 章所研究的 OPC 通信方式，方便地集成第三方人机界面，从而提高系统的灵活性。该方式主要应用于水处理、食品饮料等行业。

（2）控制 ＋ 数据处理

这种方式充分发挥了 PC 机的计算与数据处理性能，完成复杂、快速的控制算法，适用于复杂配方系统、批处理系统。该方式多用于数据自动记录、检测分析、仓储物流等行业。

（3）运动控制 ＋ 视频系统 ＋ 快速 I/O

通过 C/C++接口与第三方的运动控制和视频系统的软硬件相集成，以及与第三方的快速 I/O 模块集成，完成快速运动控制。主要用于汽车行业、包装机械、装瓶机等行业。

（4）控制 ＋ 企业办公系统

通过标准化接口如 OPC、ActiveX 直接与企业办公自动化软件 Excel、Access 相连，同时连接工业控制网络与办公网络，为企业资源计划（ERP）和制造执行系统（MES）提供实时的过程数据。还可连接企业内部网甚至国际互联网，为企业的电子商务提供准确及时的生产数据。

目前 PCBCS 系统在国内的应用没有国外广泛，主要原因是人们对传统 PLC 系统的可靠性能坚信不移，而基于 PC 的自动化控制系统这种新鲜的概念则还需要一段时间才能被人们所认同和采纳。

4.2 WinAC系统组成

西门子公司的解决方案：SIMATIC WinAC（视窗自动化中心）就是基于 PC 的自动化控制系统产品的代表之一。根据功能需要，WinAC 提供了以下组件：

（1）Windows Logic Controller（WinLC）控制组件，使得个人电脑（PC）可

作为可编程逻辑控制器（PLC）运行 PLC 程序。它使用西门子硬件 PLC 的标准设计开发环境 SIMATIC STEP 7 进行组态、编程和维护，并且 SIMATIC S7-PLC 与 WinAC 可方便的互相转化。

（2）WinAC 计算/可视化（Computing/Visualization）组件，提供了各种标准接口（如 ActiveX、OPC 等），可通过标准应用程序如 Excel、Visual Basic、Visual C++或 HMI 监控过程数据。

（3）WinAC Tool Manager 工具管理器，提供了一个控制应用程序的中心，用户可以把应用程序的快捷方式放置于这个工具栏上，通过键盘可选择需启动的应用程序。

（4）网络功能，提供了 CP 5611、CP 5613 通信板卡的驱动。

（5）SIMATIC WinAC ODK（开放的开发工具包），可集成运动控制、视频系统、数据库应用以及用户开发的 C/C++程序，为扩展系统功能和实现特殊控制要求提供了接口。

WinAC 包括三种类型产品：

WinAC Basis 基本型，运行于标准 Windows NT。它适用于除控制任务外还有大量的 PC 任务的场合，用于组成对实时性和相应时间的要求不高的系统，成本较低。

WinAC RTX 实时型，基于 Microsoft Windows NT 实时扩展内核 VenturCom，是针对具有确定性能的控制任务、运动控制、视频控制、快速 I/O、快速闭环调节的解决方案。

上述两种都属于软件型 WinAC，而 WinAC Slot 插槽型则属于硬件型 WinAC。它置于 PC 的 PCI 扩展总线插槽中，其控制任务可独立于操作系统，操作性能和指令集基于 S7-400 CPU，与 CPU412/416 性能相同，且板卡上集成了 MPI、DP 通信口，无需再单独购置通信板卡。插槽型 WinAC 还提供了电源扩展板选件，用于提供独立于 PC 机电源的供电，确保在 PC 机断电后仍能正常运行。存储卡选件可对处理器数据进行保持，需电池供电。可见，插槽型 WinAC 适用于对确定性、实时性、高可靠性有较高要求的场合。

4.3 WinAC 系统典型配置[43][45][46]

WinAC 系统是一个具有多种标准接口的开放的系统，它的应用也多种多样，可根据实际需要选择合适的配置。

（1）基于本地连接的 WinAC 系统配置

基于本地连接的 WinAC 系统可使用内部接口或 OPC 接口，与本地 HMI 进行通信，并通过 PROFIBUS-DP 总线控制远程 I/O 模块。

内部接口方式的连接如图 4.3.1 所示。WinCC、Protool/Pro 监控软件通过内部接口与 WinAC 系统交换数据，实现监控功能。WinAC Computing 提供的 ActiveX 控

件使用户可用于自行开发 PC 应用程序，增强了系统的灵活性。对于基本型 WinAC 和实时型 WinAC，需要在 PC 机上插入 CP 通信卡，将 WinAC 数据通过 PROFIBUS 现场总线传递到远程 I/O 设备；若用插槽型 WinAC，则可直接利用它本身提供的 PROFIBUS-DP 接口，将数据传递到远程 I/O 设备。

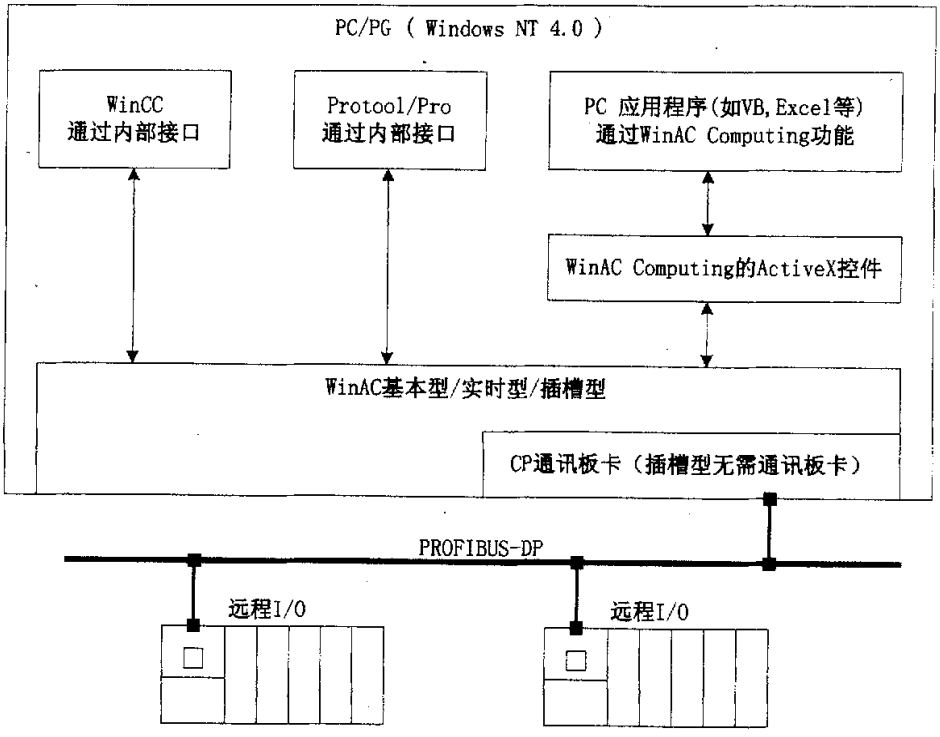


图 4.3.1 基于本地连接的 WinAC 系统配置：内部接口方式

OPC 接口方式的连接如图 4.3.2 所示。该方式下，WinCC、Protool/Pro 监控软件通过 WinAC Computing 提供的 OPC 服务器与 WinAC 系统交换数据，实现监控功能。也可开发第三方的 OPC 应用程序与 WinAC 系统交换数据。

另外通过 SIMATIC NET，可实现与 WinAC OPC 服务器的基于 MPI/DP/Ethernet 连接的 S7 通信（S7 通信是 S7 系列 PLC 基于 MPI、PROFIBUS、Ethernet 网络的一种优化的通信协议，主要用于 S7-400/400、S7-300/400 PLC 之间的主－主通信，也非常适合 S7 PLC 与 HMI 通信，如与操作面板 OP/TP 以及上位机监控软件的通信）。

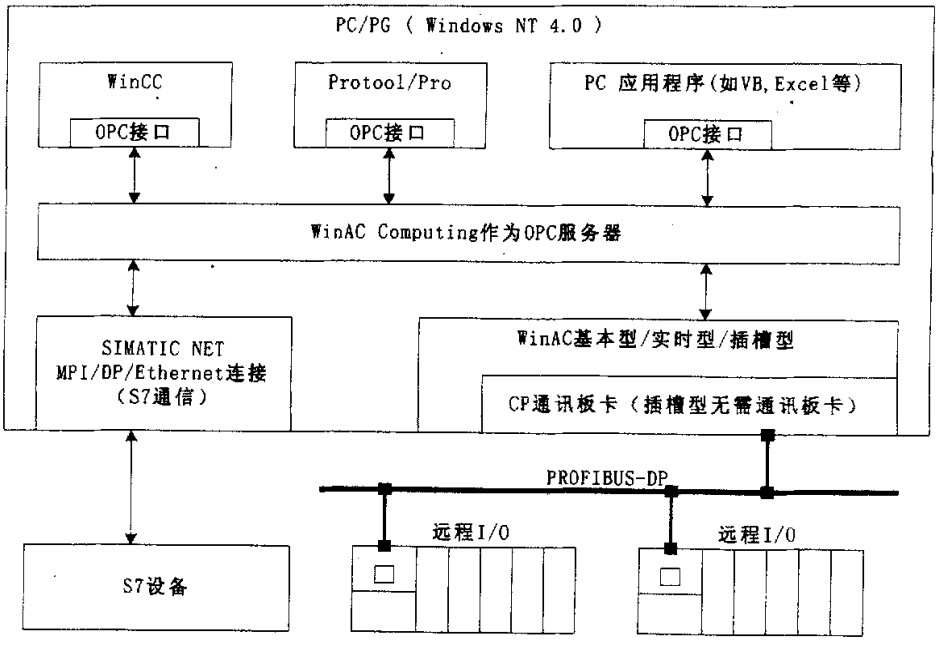


图 4.3.2 基于本地连接的 WinAC 系统配置：OPC 接口方式

（2）基于以太网连接的 WinAC 系统配置

基于以太网连接的 WinAC 系统可通过 WinAC Computing 提供的 ActiveX 控件或 OPC 接口对 WinAC 系统进行远程监控等操作。ActiveX 控件连接方式如图 4.3.3 所示。

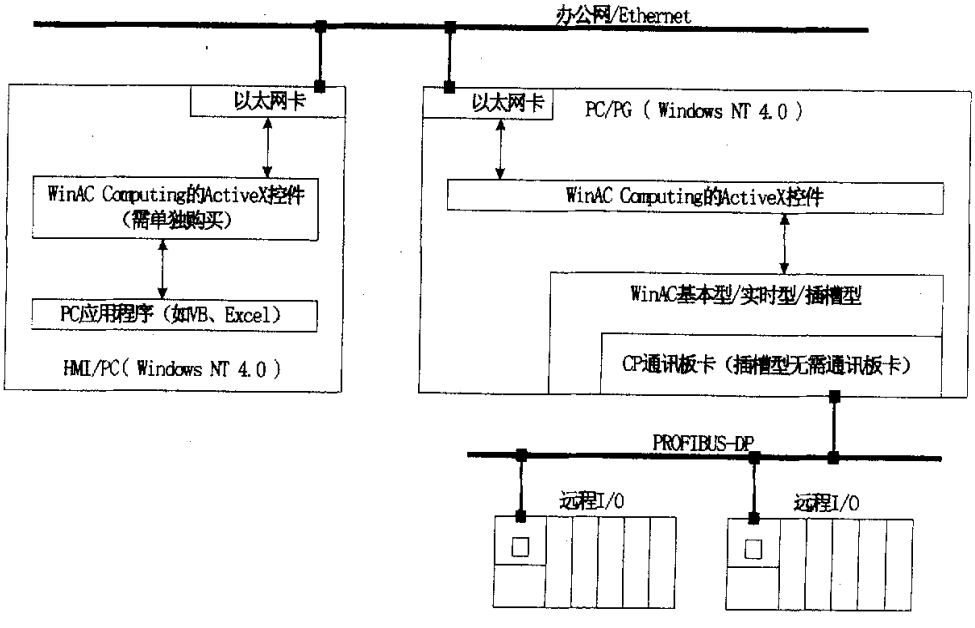


图 4.3.3 基于以太网连接的 WinAC 系统配置：ActiveX 方式

可见通过以太网，WinAC 系统的生产数据可连接到办公网络，因此该方式为远程监控 WinAC 控制系统提供了途径，在办公室即可掌握现场设备数据。

OPC 连接方式如图 4.3.4 所示。同样可通过以太网远程访问 WinAC 系统，监控现场设备数据，然而上述ActiveX控件连接的方法中在客户端需购买专门的ActiveX控件。

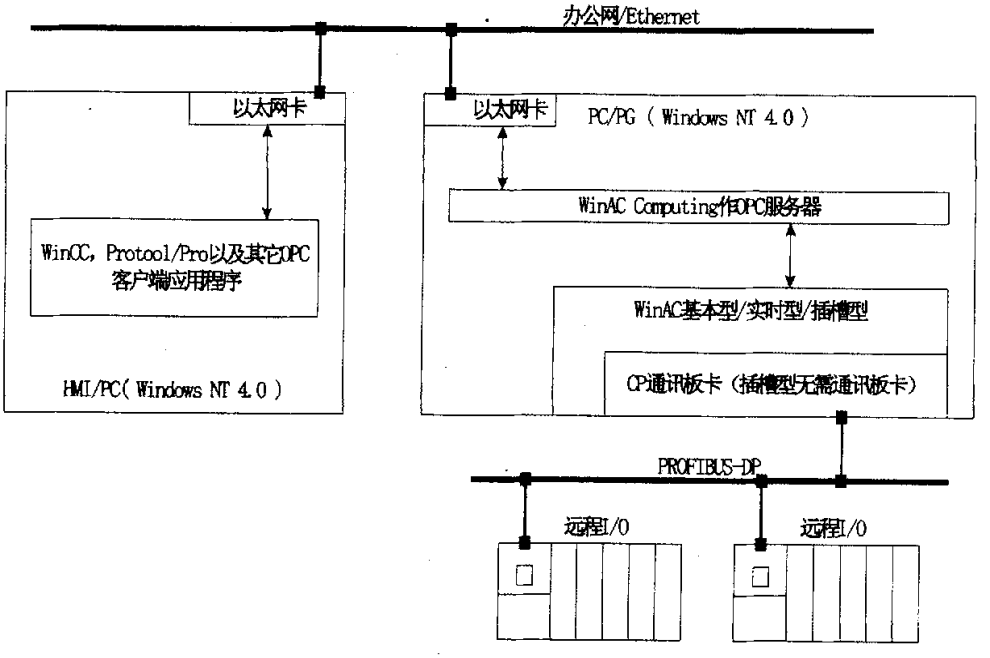


图 4.3.4 基于以太网连接的 WinAC 系统配置：OPC 方式

4.4 WinAC Basis 系统的软件接口研究

WinAC 系统提供了与 Office、VB、VC 等第三方工具的标准接口，为扩展系统功能提供了可能性。作者对 WinAC Basis 基本型的 Excel 接口、OPC 接口以及 C/C++ 编程接口进行了较深入的研究。

4.4.1 WinAC 的 OPC 接口的研究与应用

WinAC 系统提供了 OPC 服务器供其它客户端程序访问。WinAC 3.0 版本支持 Computing OPC 服务器，4.1 版本则开始支持 SIMATIC NET OPC 服务器，以提供更好的数据访问性能。Computing OPC 提供数据存取访问（DA）服务，而 SIMATIC NET OPC 除提供数据访问服务之外，还提供报警和事件（A&E）服务[41][42]。

WinAC 系统 OPC 接口的应用可分为控件方式和客户端代码方式。可以利用西门子公司发布的控件 WinAC Computing 控件与 WinAC Net OPC 控件实现 OPC 客户端。由于这些控件已经封装了与 OPC 服务器通信的代码，提供对 WinAC 系统读/写操作的方法，并提供了相应的错误处理功能，在高级语言中很容易使用这些控件。用这种方法开发 WinAC 系统的 OPC 客户端，开发周期短，可靠性高，但灵活性不够，因

为用户只能使用控件已提供的有限的事件与方法。另一种开发WinAC系统客户端应用程序的方法就是编写客户端代码，从连接OPC服务器、添加组、添加数据项直到事件处理都需自行编写处理代码。这种方法灵活性较大，但工作量比控件方式要大的多，且处理不当会引发程序异常，影响客户端的可靠性。

对于WinAC Basis 3.0系统的Computing控件方式的使用，将会在4.4.2节中阐述，这里研究它的客户端代码方式在VB 6.0中的应用。

所有OPC客户端开发的过程大同小异，都必须按照3.5.3小节中的OPC通信初始化流程进行通信前的准备。前面章节已经研究了S7-200的OPC客户端应用程序开发技术，本节仅提出需要开发WinAC的OPC客户端应用程序时注意的不同之处。不同的只有两项内容：一是服务器名称；二是数据项名称。此外，还需设置“Computing Configuration”，将其OPC的“Control Engine”设置为“WinLC”，否则无法与WinAC系统建立连接。

在VB 6.0中先要引用“SIEMENS OPC DAAutomation 2.0”自动化数据访问组件，然后即可方便地开发客户端程序。连接WinAC Computing OPC服务器：

```
Set MyOPCServer = New OPCServer
Call MyOPCServer.Connect("OPCServer.WinAC")
```

添加数据项，须按服务器规定的数据项名称填写。可按数据项数组的形式添加，如：

```
Set MyItems = MyGroup.OPCItems
ItemIDs(1) = "2,M0.0,BOOL"
.....
ItemIDs(10) = "2,MW20,WORD"
Call MyItems.AddItems(10, ItemIDs, ClientHandles, ServerHandles, Errors)
```

也可添加单个数据项，如：

```
MyGroup.OPCItems.AddItem "M0.0:BOOL", 1
MyGroup.OPCItems.AddItem "MW2:WORD", 2
```

WinAC Computing OPC支持同步/异步方式读写变量，当服务器数据改变时自动产生回调（Recall）事件，这与3.5.3节中研究的S7-200 OPC的方法是相同的。由此，可体会到OPC规范的标准化给用户带来的巨大效益：用户无需针对不同的设备或系统，花费大量时间去研究硬件设备的底层，只需按照OPC规范编写应用程序，连接到不同的服务器即可获得服务器数据。

4.4.2 Excel接口的研究与实现

WinAC Computing提供的ActiveX控件“S7Data”可将软件PLC：WinLC中的过

程数据采集到 Excel，并可用 Excel 的宏命令（macros）将数据保存在电子表格中。在 Excel 中采集 WinLC 中的数据可有三种方式：手动方式、周期方式以及时间触发方式。

在 Excel 中访问 WinLC 需要在 VBA 编程环境下编写相应代码，首先必须启动 VBA 编程环境 Visual Basic 编辑器，并引入 S7Data 控件（S7Data1）。它提供了 ReadVariable 方法：

ReadVariable（*VariableName* as String, *Value*, *State* as Long, *TimeOut* as Long）。

其中，*VariableName* 是变量名，如要采集 MB6 的值，则 *VariableName*="MB6" 即可；*Value* 是变量的值；*State* 是变量的状态；*TimeOut* 用于设置读变量超时时间。

不管手动方式还是周期方式，由于数据采集都可由同一过程完成，故可在 VB 程序模块（Module1）中设计一个 ShowNewData()过程用于采集变量当前值。

（1）手动方式，即每次数据采集均需人工干预。这种方式是最基本、最简单的了，只需将 ShowNewData 过程与特定用户事件如按钮单击事件（Click）关联即可。

（2）周期方式，即周期地自动采集 WinLC 中的数据。可在先前建立的模块 Module1 中编写周期性调用的过程 PeriodData ()，如下所示：

```
Global NextTime As Variant
Sub PeriodData()
NextTime = Now + TimeSerial(0, 0, Val(MainFrm.timeBox.Text))
Call ShowNewData
Application.OnTime NextTime, "PeriodData"
End Sub
```

此时用到了 VBA 提供的 OnTime 事件：

Application.**OnTime**（*EarliestTime*, *Procedure* as String, *LatestTime*, *Schedule*）

其中，*EarliestTime* 为过程开始运行的时间；*Procedure* 为要运行的过程名；*LatestTime* 是可选参数，表示过程开始运行的最晚时间；*Schedule* 也是可选参数，若为 True 则安排一个新的 OnTime 过程。如果为 False 则清除先前设置的过程，默认值为 True。

（3）事件触发方式。这种方式下的数据采集需要设置 S7Data1 控件的事件（Events）属性，如图 4.4.2.1 所示，同时可设置数据更新周期和死区。

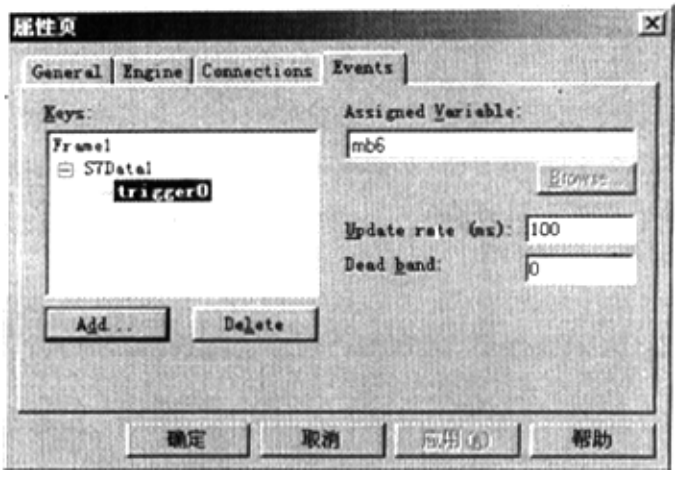


图 4.4.2.1 设置控件事件属性

当所添加的变量值发生变化时，可在 S7Data1 控件的 ValueChanged 事件中捕获到，如下所示：

```
Private Sub S7Data1_ValueChanged(ByVal Property As String, ByVal VarName As String, ByVal Value As Variant, ByVal Quality As Integer)
Select Case Property
Case "trigger0"
Call ShowNewData
End Select
End Sub
```

这三种方式都可采集 WinLC 中的数据，前两种方式下，可在宏的运行期定义需采集的变量名，第三种方式则需在设计期定义变量名。运行效果如图 4.4.2.2 所示。

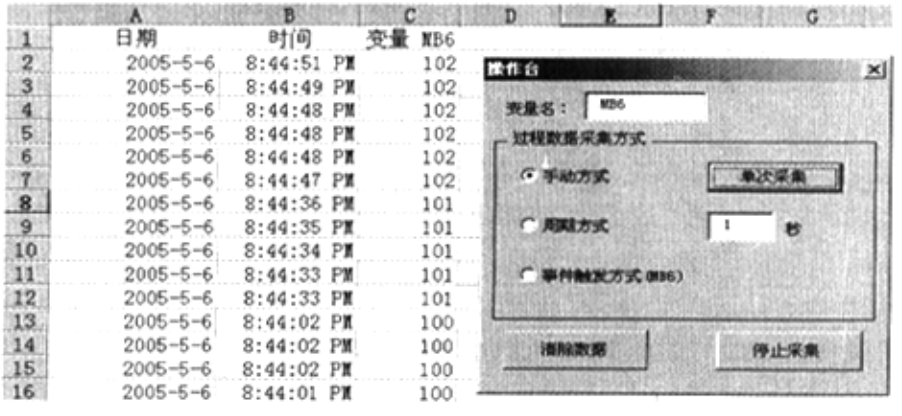


图 4.4.2.2 WinAC 的 Excel 接口的应用

4.4.3 C/C++编程接口的研究与实现

WinAC Basis ODK 3.0 为 WinAC Basis 3.0 提供了开放的开发工具，它包含以下组件：WinLC 3.0 的 COM 扩展组件；Visual C++ 6.0 应用向导；用于与 COM 对象交换数据的 STEP 7 系统功能块（SFB65001、SFB65002）等，从而使 WinAC 系统可以集成用户 C/C++代码。它应用了微软的 COM 技术，将用户开发的 C/C++程序作为 COM 对象，以 DLL 的形式装载到 WinLC 中。用户可创建多个 COM 对象；每个 COM 对象又可以包含多个命令。

在 WinAC 系统中 STEP 7 程序可执行由 C/C++代码编写的三种功能代码：同步（Synchronous）功能、异步（Asynchronous）功能、监视（Monitoring）功能。

（1）同步功能

在 OB1 主循环中，C/C++程序编写的同步功能代码在 STEP 7 程序中通过系统功能块 SFB65002 调用，需占用 OB1 主循环周期中的一段时间，如图 4.4.3.1 所示。只有当 C/C++程序处理完毕，SFB65002 的调用过程才终止，然后再继续执行接下来的 STEP 7 程序。这种同步方式适合于实现较复杂的算法功能，但它不适用于那些执行时间不确定的处理过程。

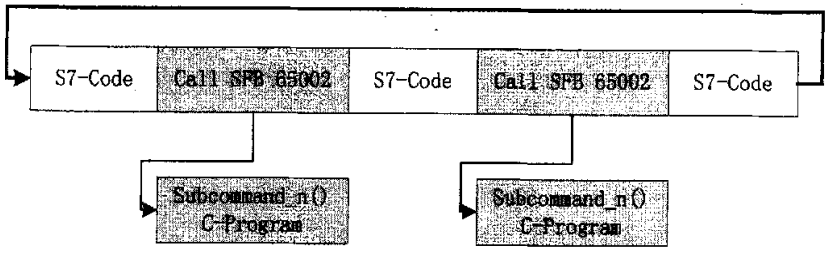


图 4.4.3.1 同步功能示意图

（2）异步功能

异步功能适用于磁盘读写等低速执行过程。执行过程如图 4.4.3.2 所示。

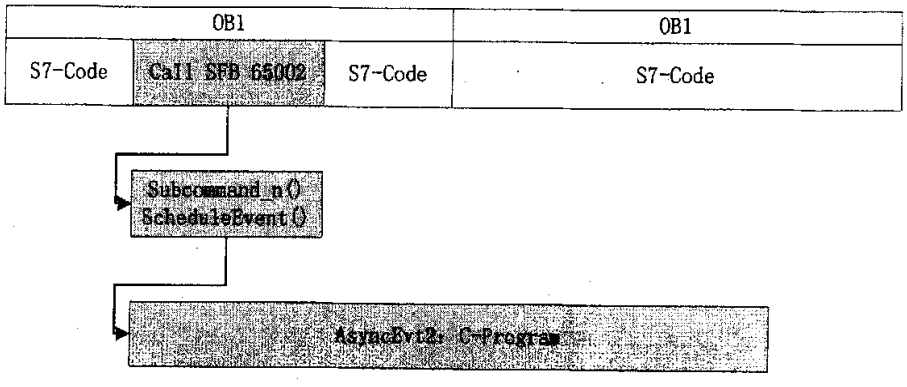


图 4.4.3.2 异步功能示意图

实现异步功能的程序由 ODK 同步功能函数 ScheduleEvent 启动：

```
AsyncEvent_1 *AsyncEvt2 ;
Processor.ScheduleEvent ( AsyncEvt2 ) ;
```

异步功能在异步事件中实现：

```
long AsyncEvent_1::Execute ( ) ;
```

此后，异步程序与 OB1 主程序并行，直至异步程序结束。

（3）监视功能

启用监视功能后，C/C++程序以多线程的形式与 OB1 并发执行，并监视外部事件或 C/C++程序的执行状态。当事件触发时，C/C++程序将通过 ScheduleOB 函数调用 WinAC 中的组织块 OB40。如图 4.4.3.3 所示。

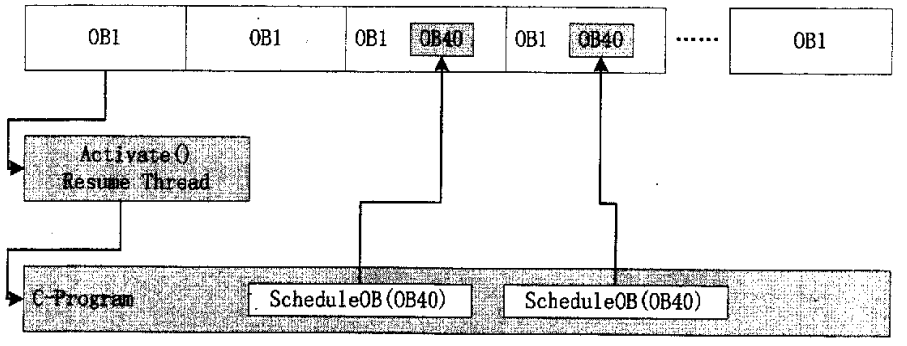


图 4.4.3.3 监视功能示意图

上述三种功能均可由 WinAC Basis ODK 提供的集成在 Microsoft Visual C++ 6.0（VC++ 6.0）中的向导（如图 4.4.3.4 所示）创建，并在生成的框架内填写相应的代码，以完成 COM 对象设计。

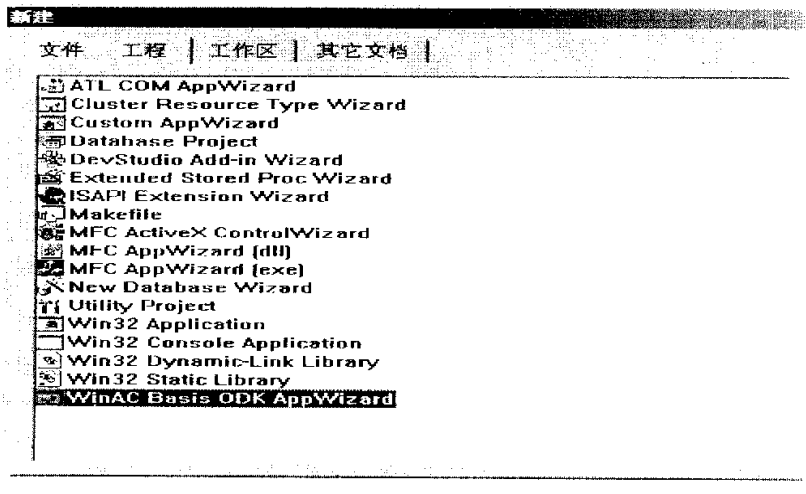


图 4.4.3.4 在 VC++ 6.0 中应用 WinAC ODK 向导

在 VC++ 6.0 中，创建 WinAC Basis 系统的 COM 对象，构建它的同步功能框架

（必选），并可进一步定义同步函数个数、名称，如图 4.4.3.5 所示。

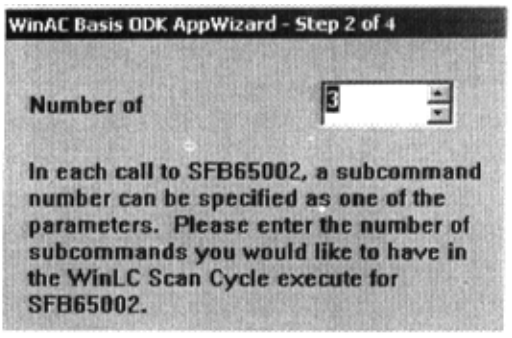


图 4.4.3.5 创建同步函数

与此相似，再根据需要构建异步功能框架（可选）和监视功能框架（可选），并可进一步定义函数个数、名称。至此，COM 对象设计框架已构建完毕，还需在相应函数中填写相应代码。

对于本节创建的 COM 对象的同步功能，需在函数 SUBCOMMAND_1、SUBCOMMAND_2、SUBCOMMAND_3 中实现。如图 4.4.3.6 所示。

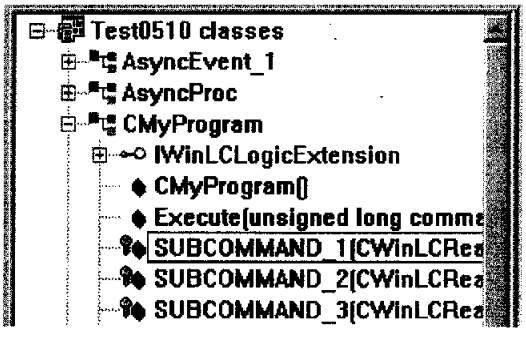


图 4.4.3.6 同步函数

异步功能需在异步事件 AsyncEvent_1 的 Execute 函数中实现，如图 4.4.3.7 所示。

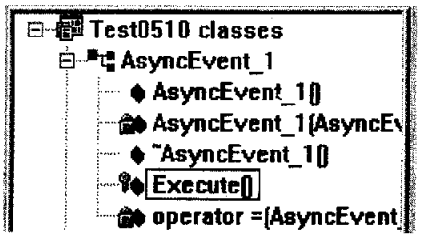


图 4.4.3.7 异步函数

监视功能需在 Monitor_1 对象的 Excecute 函数中实现，如图 4.4.3.8 所示。

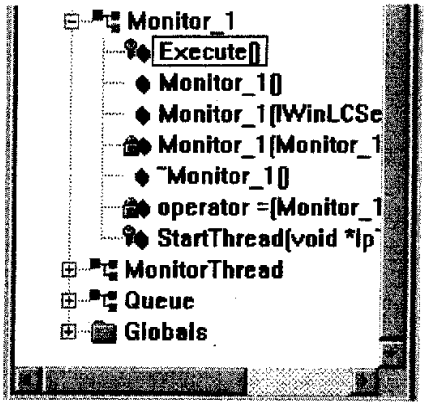


图 4.4.3.8 监视函数

这些功能都可用 C/C++进行开发，本节不再赘述 VC++ 6.0 环境下的 C/C++程序开发细节。代码编写完毕，即可编译源程序，编译无误后可生成 DLL 文件。在生成 DLL 文件时，VC++ 6.0 已将该 DLL 文件注册成 COM 对象，并提供了唯一的“ProgID”标识该 COM 对象，若要改变该 DLL 文件在磁盘中的位置，则需重新注册。然后，便可在 STEP 7 中调用该 COM 对象了。一般在暖启动组织块 OB100 中调用 SFB65001（“CREA_COM”）创建 COM 对象，而后在 OB1 主循环中调用 SFB65002（“EXEC_COM”）执行该 COM 对象。

OB100 中调用 SFB65001 如图 4.4.3.9 所示。

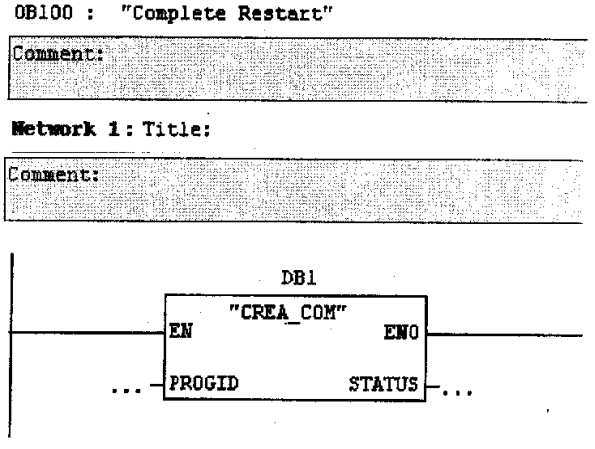


图 4.4.3.9 调用 SFB65001

在 OB100 程序中调用系统功能块 SFB65001 初始化该对象时，需提供“ProgID”，因为每台计算机上可存在多个 COM 对象，它们之间是通过唯一的“ProgID”互相区别的。可在 VC++工程的资源文件（*.rgs 文件）中查看到该“ProgID”的值，即为下图 4.4.3.10 中的选中部分：“Test0510.MyProgram”。

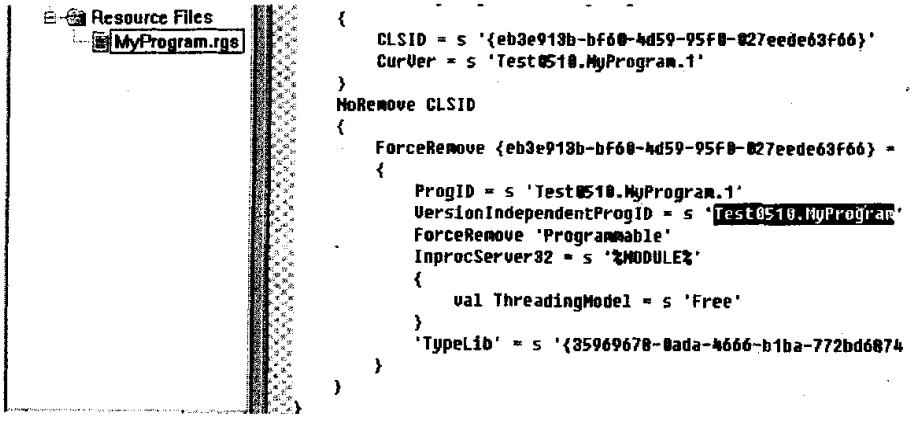


图 4.4.3.10 查看 ProgID

在 SFB65001 的背景数据块 DB1 中填写 ProgID，如图 4.4.3.11 所示。

	Address	Declaration	Name	Type	Initial value	Actual value
1	0.0	in	PROGID	STRING [254]	''	'Test0510.MyProgram'
2	256.0	out	STATUS	WORD	W#16#0	W#16#0

图 4.4.3.11 将 ProgID 参数写入 DB 块

在 OB1 中调用 SFB65002，如图 4.4.3.12 所示，以执行 COM 所封装的算法。

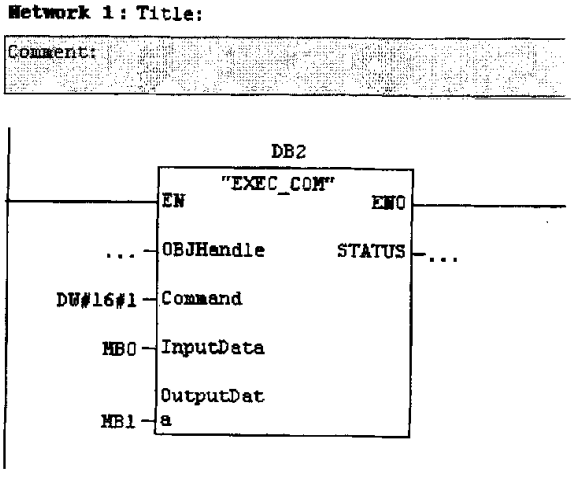


图 4.4.3.12 调用 SFB65002

Command：DWORD 类型，指定 SFB65002 调用的同步功能函数编号；

InputData：ANY 类型，指定输入数据区；

OutputData：ANY 类型，指定输出数据区。

至此，本节研究探讨了应用 VC++ 6.0 开发 COM 对象，并在 STEP 7 中调用该 COM 对象的方法，下面将通过电梯群控教学系统的设计，研究 C/C++编程接口以及前面章节中讨论的通信技术、OPC 接口技术在 WinAC Basis 系统中的综合应用。

4.5 基于WinAC Basis的电梯群控教学系统设计

4.5.1 电梯群控系统简介[60][61][62]

目前，在许多高层建筑中，为满足交通的需要，通常安装了多部电梯，这就需要采用一种管理多部电梯协调运行的控制系统即电梯群控系统（EGCS），提高电梯群的运行效率和服务质量。电梯群控的主要功能是调度和管理各部电梯，指定电梯服务楼层，这对改变原先由于电梯的单独控制而造成的楼层分布不均，资源浪费，电梯损耗不均匀等状况有利。因此，电梯群控对于改善电梯的运行效果，具有十分重要的作用。

电梯群控智能系统的发展大约已有半个世纪，最早是由日本Toshiba公司提出的。1949年，纽约联合国大厦首次使用了继电器逻辑组成的电梯群控系统，经历了由当初的预选控制到后来的分区控制。随着电梯功能的进一步完善及计算机控制技术的发展，电梯群的控制已进入了一个新的发展阶段：智能控制。所谓电梯群的智能控制就是寻求优化的控制策略，优化调度多部电梯以提高电梯的运行效率和服务质量，从而尽可能的减少乘客的侯梯时间，从整体上提高梯群的客流输送能力。国际上各大电梯公司相继推出了一些控制算法，如：日本Mit subishi公司的综合分散度群控方法、Hitachi公司的时间最小/最大群控方法，瑞士Schindler公司的综合服务成本群控方法，美国Otis公司的相对时间因子群控方法等。

不管采取何种控制算法、基于何种控制理论（专家系统、模糊理论、神经网络等），平均候梯时间的最小化是一个共同的也是最基本的控制目标。

4.5.2 方案设计

目前多数电梯群控系统采用PC+PLC控制结构，多台PLC分别控制各部电梯运行，PC机则完成监控任务，这是比较传统的设计方法，也是比较安全可靠的。随着基于PC的控制方案的提出，也有人提出WinAC+ET200（远程I/O）的设计方案。这种方案可将控制、监控等任务置于PC机上执行，而每组远程I/O对应于每台电梯，降低了设计成本，然而当PC出错（如死机）时，电梯安全则成为显著的问题。本文提出WinAC+S7-200的设计方案，由WinAC负责电梯群控调度，每台S7-200 PLC对应控制每台电梯，这样即使PC机出错，也可由S7-200 PLC保证电梯运行的安全性。该方案仅用于了教学实验，展示WinAC系统的C/C++编程接口和OPC接口的应用。

本节设计的电梯群控系统共有三台五层电梯参与群控。每台电梯的内选信号（选层、开门/关门）由各CPU 224采集，并接受CPU 224输出的控制信号，如运行/停止、上行/下行、开/关电梯门等。电梯厅外呼叫信号一般有两种方式:集选呼叫和非集选呼叫。集选呼叫，即大厦每一层只有一个呼叫板，乘客的外呼请求信号由该采集板统一采集送给群控系统进行分析并派梯。非集选呼叫，即大厦每一层各

台电梯有各自的呼叫板，乘客可选定任一电梯请求服务，但系统仍将该信号送至群控模块进行处理，确定由哪台电梯响应乘客的请求。在该系统中采用了集选呼叫方式。三台电梯在每层共用一组大厅外唤按钮（上/下按钮），大厅外唤信号依次分配到各 PLC 输入点。

对于楼层的定位，采用目前电梯系统中普遍使用的脉冲计数方法。当电机带动电梯运动时，通过光电转换装置，由其发出的脉冲数可确定电梯当前位置。假设当电梯停在 1～5 层时，对应脉冲数分别为 100、200、300、400、500。为方便控制电梯停靠某一层，故设定减速区域为 10 个脉冲大小，如图 4.5.2.1 所示。对于开/关电梯门的定位，也采用脉冲计数方法。

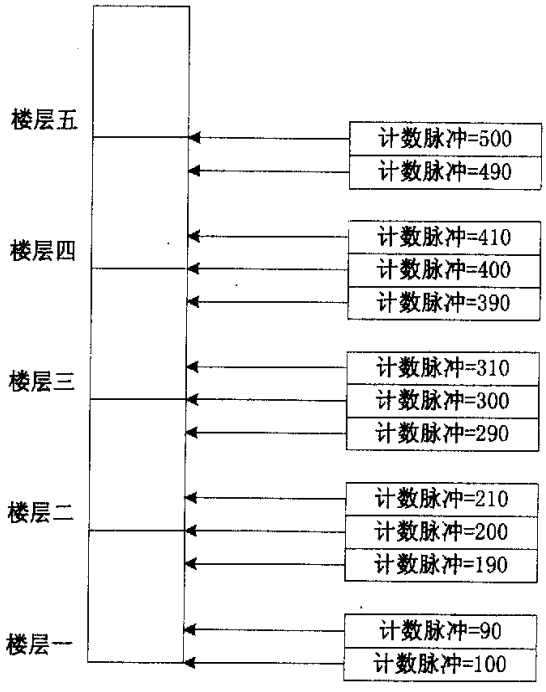


图 4.5.2.1 电梯运行脉冲计数法

控制算法由控制/监控计算机完成。控制计算机安装有软件：PLC 编程软件 STEP 7 V5.2、WinAC Basis 3.0（软 PLC）、WinAC Basis ODK 3.0(C/C++接口开发包)、监控软件 Protool/Pro；PC 机插有 CP 5613 通信卡。

由于实验室没有实际的电梯对象，因此用 OPC 接口编写虚拟电梯对象。被控对象计算机与 CPU 224(1/2/3)通过 PPI 电缆交换数据（V 区），从而与控制/监控计算机交换数据。

系统连接图如图 4.5.2.2 所示。

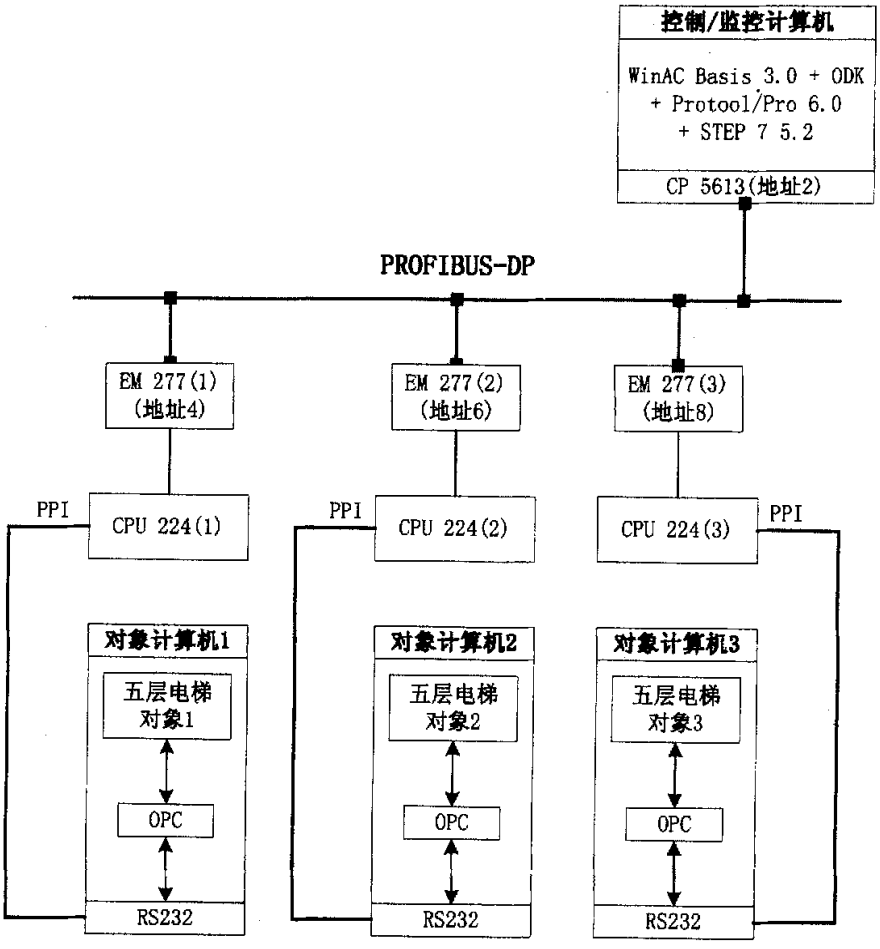


图 4.5.2.2 电梯群控系统连接图

4.5.3 资源分配与硬件组态

每台 S7-200 PLC 需采集的信号有：电梯内选信号（层按钮信号、开/关门信号）、楼层计数脉冲信号、开关门计数脉冲信号、载重量信号、大厅外呼信号（为节省 I/O 点数，将集选信号分配到每台 S7-200 PLC）；需输出的信号有：电梯运行/停止信号、电梯上行/下行信号、电梯开/关门信号、电梯速度控制信号等。

鉴于此，在 STEP 7 中进行硬件组态、分配数据交换区时，需考虑到资源分配问题，以充分利用 S7-200 PLC 的 I/O 及存储区域资源。

在 STEP 7 中硬件组态前，需先安装 EM 277 模块的 GSD 文件（电子设备数据文件）“SIEM089D.GSD”，此后才可组态从站。GSD 文件将不同厂家生产的 PROFIBUS 产品集成在一起，给出这些产品的功能参数（如 I/O 点数、诊断信息、波特率等）。在组态时，用组态工具可装入每个设备的 GSD 文件，这就意味着用户可以方便地将不同厂商生产的 PROFIBUS 设备集成在同一 PROFIBUS 系统中。GSD 文件由每种类型

设备的制造商准备，对每一种设备类型的特性，用一个确切定义的格式作了明确而全面的描述，并以电子设备数据单的文件形式向用户提供。这种确定的文件格式允许组态系统方便地读入任何 PROFIBUS 设备的 GSD 文件，并在组态总线系统时自动地使用这些信息。

将 PCStation 站的 DP 地址定义为 2，将三个从站的 DP 地址依次定义为 4、6、8。在 EM 277 模块上必须进行相应的拨码操作，使硬件设置与硬件组态的地址一致。硬件组态如图 4.5.3.1 所示。

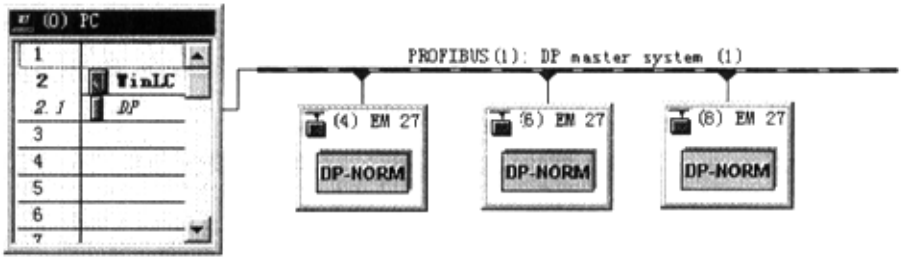


图 4.5.3.1 电梯群控系统硬件组态图

对于每个从站，都可设置 S7-200 PLC 中用于数据交换的 V 区的偏移地址（I/O Offset），若默认为 0，则代表从 VB0 开始，如图 4.5.3.2 所示。

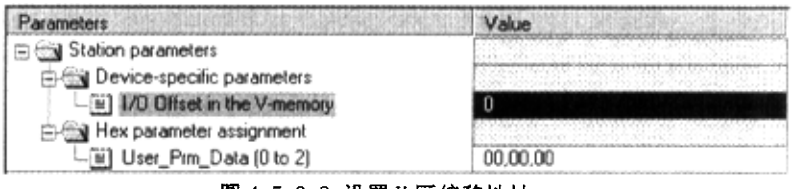


图 4.5.3.2 设置 V 区偏移地址

数据交换区的长度与插入从站的输入/输出模块的 I/O 点数有关，若为“8 Bytes Out/8 Bytes In”（如图 4.5.3.3 所示），则 VB0～VB7 为接收数据区，VB8～VB15 为发送数据区。其它从站的组态与此相似。

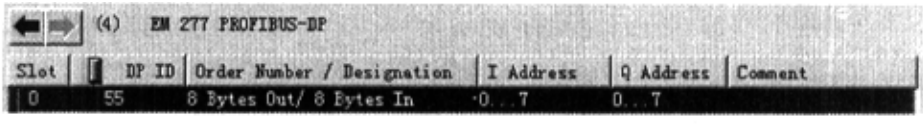


图 4.5.3.3 配置从站输入/输出模块

WinAC 与 S7-200 PLC 数据交换区对应关系如图 4.5.3.4 所示。

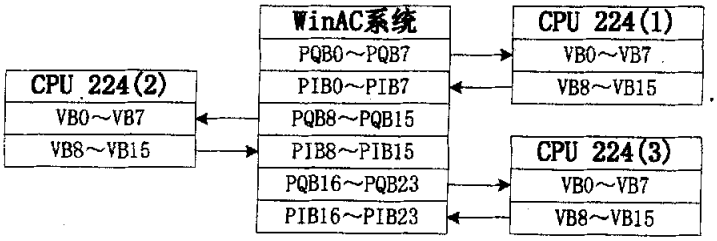


图 4.5.3.4 WinAC 与 S7-200 PLC 数据交换区对应关系

4.5.4 控制程序设计

在设计电梯群控系统控制部分时，为了使系统具有良好的灵活性、可操作性以及可扩充性，系统采用模块化的设计思想，系统的各种功能由相应的模块实现。

（1）信号采集模块

该模块由 S7-200 PLC 完成电梯内选信号和大厅外呼信号的采集。

（2）调度算法模块

该算法根据最小候梯时间原则，分析乘客请求信号，决定派哪台电梯响应乘客请求。应用 VC++ 6.0 编写成 DLL，作为 COM 对象由 WinAC 调用该算法。

由于该系统主要用于演示WinAC与S7-200 PLC之间的通信及其C/C++编程接口和OPC接口的应用，因此这里的调度算法仅采用了最小候梯时间原则，即由大厅外呼信号和各电梯当前运行状态、厢内按钮情况，分别计算每部电梯响应完梯内请求为止，再从最后停靠楼层运行到外呼信号所在楼层所需时间t1，t2，t3，派出计算结果最小的电梯响应该外呼信号[53]。其中t1，t2，t3的计算如下，假设下列变量：

N1：外召唤所在的层；N2：电梯在外召唤到来时的当前楼层；M1：电梯在本方向到达的最远停靠层；M2：电梯到达的本方向后方的最远停靠层；T1：电梯以额定匀速行驶途经一层所需的时间；T2：电梯加减速、开关门和停止的平均时间；N：电梯运行到召唤楼层响应梯内请求信号及外召唤所停的层站数。

A.外呼信号的方向与电梯当前运行方向同向，且在电梯方向的前方时，电梯运行过程示意图如图 4.5.4.1 所示。

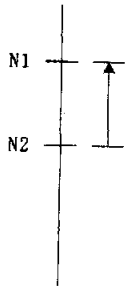


图 4.5.4.1 外呼信号方向与电梯当前运行方向同向且在电梯方向的前方

此时响应时间 t=｜N1-N2｜·T1+N·T2-N·T1

B.外呼信号的方向与电梯当前运行方向反向时，电梯运行过程示意图如下：

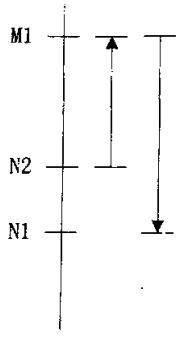


图 4.5.4.2 外呼信号方向与电梯当前运行方向反向

此时响应时间 t=(｜M1-N1｜+｜M1-N2｜)·T1+N·T2-N·T1

C.外呼信号的方向与电梯当前运行方向同向,且在电梯方向的后方时，电梯运行过程示意图如下：

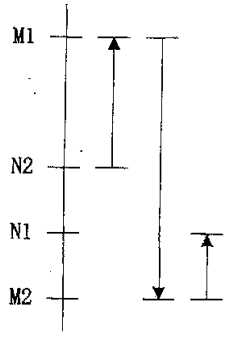


图 4.5.4.3 外呼信号方向与电梯当前运行方向同向且在电梯方向后方

此时响应时间t=(｜M1-N2｜+｜M1-M2｜+｜M2-N1｜)·T1+N·T2-N·T1

调度算法流程图如图4.5.4.4所示。

（3）安全保护模块

当WinAC系统出错时，CPU 224（1）、CPU 224（2）、CPU 224（3）可接管电梯控制权，将梯内乘客安全送达请求的楼层。WinAC每500ms给从站发送一个联络信号，若从站接收不到该周期信号，则认为PC机出错，接着执行安全保护模块。该模块由WinAC与S7-200 PLC完成。

（4）速度控制模块

速度控制模块实现电梯加减速控制。给定当前层和将到达的层，输出速度控制信号（WORD类型）和电梯运行状态（0：停止，1：上行，2：下行）。无论上行、下行，电梯离开原位10个脉冲之内，作匀加速运动，此后匀速运动，当距离目的楼层10个脉

冲时，再作匀减速运动，直至刚好停在目的楼层。该模块由S7-200模块完成。

（5）信号输出模块

该模块负责将控制信号输出给电梯系统的执行器，完成开门/关门、上行/下行、启动/停止、改变速度等。该模块由S7-200 PLC完成。

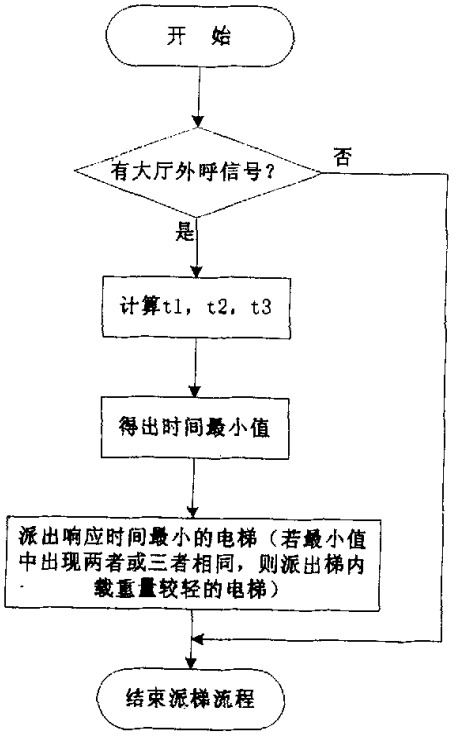


图4.5.4.4 调度算法流程图

4.5.5 监控程序设计

监控部分的设计可采用两种方案。一种是采用SIMATIC WinCC监控组态软件；另一种是SIMATIC Protool/Pro监控组态软件。

SIMATIC ProTool是用于整个SIMATIC HMI系列（TP、OP、MP等）的创新的组态软件包，由ProTool CS组态系统软件和用于过程可视化的运行系统软件ProTool/Pro RT组成。两个系统均可以在Windows 98 SE、Windows Millenium、Windows 2000和Windows NT 4.0操作系统上运行。单独的运行系统软件也可以在Windows CE设备上运行。Protool CS用于在Windows系统的组态计算机（编程器或PC）上创建项目，包括画面的设计、通信类型及参数的设置等。ProTool/Pro项目主要由用来操作和监控机器或设备的画面所组成，也可以组态更多的对象，例如：消息、归档、配方和脚本。Protool与PLC的连接可通过变量建立，操作单元将对来自PLC的值进行显示，并接受手工输入的数值。使用它提供的模拟程序，无需连

接设备就能测试项目，将不再需要在目标系统上装载项目。Protool RT 则运行由 Protool CS 设计的项目文件。Protool/Pro 不仅可设计运行于 PC 机的监控系统，且可为触摸屏、操作面板等设备提供组态设计环境，其目标文件将运行于这些 HMI 设备上，它提供了统一的编辑环境，具有系统资源占用少、简单灵活的特点。

SIMATIC WinCC 监控软件功能强大，但不适用于该教学系统，因此作者采用了小而灵活的 SIMATIC ProTool 作为该系统的监控软件。此时在 Protool/Pro CS 中需选择要组态的设备为“基于 Windows 的系统”目录下的“PC”，设置通信协议“SIMATIC S7 - WinAC V6.0”。建立变量（如图 4.5.5.1 所示），设置数据类型、数据采集周期等。组态显示画面（如图 4.5.5.2 所示）并连接到变量即可监控 WinAC 中的数据，如电梯当前运行状态、当前载重量、电梯门状态、梯内按键状态、大厅外呼信号状态等。

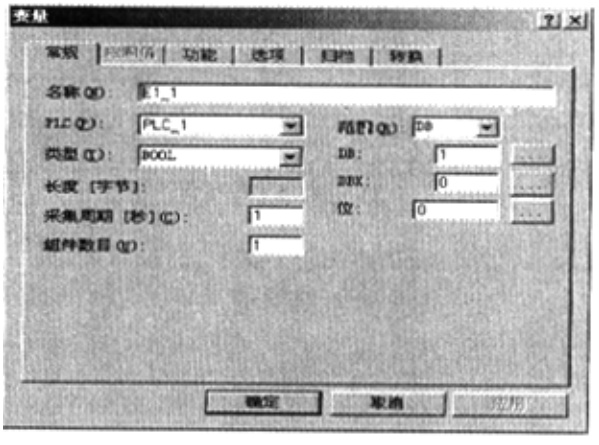


图 4.5.5.1 在 Protool 中新建变量

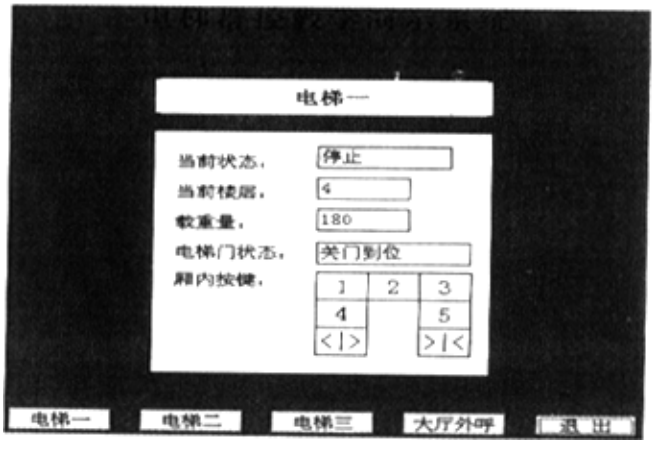


图 4.5.5.2 Protool 监控界面图

4.5.6 虚拟电梯对象设计

对于虚拟电梯对象，采用 OPC 方式与 S7-200 PLC 通信，然而无须开发三个独立的被控对象程序，因为三部电梯的 I/O 信号几乎是一致的，可通过在一个程序中设置电梯编号，以区别少数不同的 I/O 信号。虚拟电梯对象的属性有：梯内按钮、当前所在楼层、当前运行状态、当前载重量、进出乘客重量、电梯上下运行脉冲计数、电梯开关门脉冲计数。为了可改变对象运行速度，程序提供了输入域，以改变电梯运行脉冲计数速率和梯门脉冲计数速率。此外，在电梯对象中添加了大厅按钮，就免去了单独开发大厅按钮对象程序。OPC 程序的开发过程在前面章节已阐明，不再赘述。运行界面如图 4.5.6.1 所示。

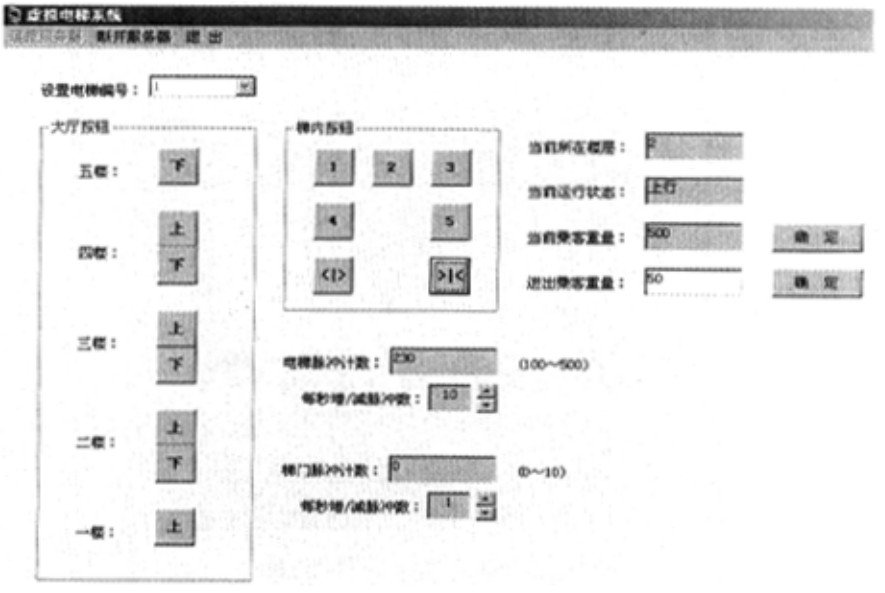


图 4.5.6.1 虚拟电梯对象运行图

该电梯群控系统实现的功能相对比较简单，还可进一步完善，如加入指定服务楼层控制、最优化速度控制、最低功耗控制、交通流量控制等。总之，电梯群控系统是一个复杂的多目标系统，可在其中实践诸多控制算法，是一个值得研究的领域。

4.6 小结

SIMATIC 基于 PC 的自动化，以 WinAC 为核心部件，将控制器、数据处理、人机界面、通信网络集成在 PC 机上，充分发挥了 PC 在处理速度、内存容量和易于扩展等方面的优势，具有很大开放性和集成度，且降低了成本。

基于 PC 的自动化具有如下优点：快速项目组态在 PC 上完成；使复杂的通信接口简单化；与 PLC/PC 上下位机的解决方案相比的价格优势；通过 PC 不断增长的性能和存储能力，提高生产率；人机界面与控制相集成的紧凑解决方案，节省了安装

空间；分布式的自动化解决方案变得简单易行；将生产过程与办公环境相集成；减少了大量连线和通信负荷。

基于 PC 的自动化现在正迅速的增长。在 PC 的帮助下，可以在一个统一的平台上真实地实现任何自动化任务，如开环和闭环控制、人机界面和运动控制。当在一个应用中，除了传统的 PLC 任务外还需要有其它 PC 的任务时，基于 PC 的自动化当是用户的第一选择。

然而传统的硬 PLC 具有自身的优点，能满足 85%～90%的控制任务，其市场占有率并不会因基于 PC 的自动化方案而陡然降低。硬 PLC 具有如下优点：可靠性无可比拟，故障停机最少；加固型结构，适合工业环境应用；对低端应用，PLC 具有极大的性能价格比优势；而且硬 PLC 也在不断提高其技术内涵，融合了 IT 技术（包括以太网、因特网、无线网技术、现场总线技术，以及运用软件工程方法开发全新的编程系统等）。

因此，在很长一段时期内，基于 PC 的自动化系统与硬 PLC 系统将会共存，并进一步融合，优势互补，从而不断增强自动化控制系统功能。

5 SIMATIC 自动化控制系统冗余技术探讨

5.1 系统可靠性及冗余技术概述

“可靠性”有广义和狭义之分。广义的可靠性是指，系统、设备或元器件在规定的条件下，在规定的时间内，完成规定功能的能力。狭义的可靠性是指，系统、设备或元器件在规定的条件下和规定的时间内，完成规定功能的概率。狭义上的可靠性的定义将“可靠性”的程度进行了量化，因此又称其为“可靠度”。为了提高系统的可靠性，在系统设计中可采用以下两种办法：一是，尽可能选用高可靠性的单元组成系统，但在设备单元方面的费用将会增加，从而使系统的造价成若干倍地提高；二是，增加一定数量的相同单元组成系统或采用多套相同的系统，即所谓冗余的方法，有效地提高系统的可靠性[22]。

冗余是指具有多余的资源，当系统中的某一部分（或整机）出现故障时，可由冗余的部分（或整机）代替故障的部分（或整机）工作，以保证系统在规定的时间内正常地完成规定的功能。冗余的资源可以是冗余的硬件、冗余的软件、冗余的信息以及重复的时间，相应地分别称之为硬件冗余、软件冗余、信息冗余以及时间冗余。硬件冗余是指系统中某个或几个关键的单元除了工作所需的基本单元外，另外设置一个或一个以上的单元，这些冗余的单元可以与工作单元同时工作，也可以处于等待工作状态，一旦工作单元出现故障，冗余单元就可代替故障的单元继续运行。软件冗余通常是针对计算机系统而言，将关键的软件复制多份存储。信息冗余也称功能余度，利用各传感器或各种系统之间存在的已知函数关系产生冗余信息，从而用以检测、识别故障。时间冗余是重复执行某段程序甚至整个程序，检测故障或使系统从故障中恢复工作。以上几种冗余类型又可根据其冗余资源是否与工作部分同时工作而分为工作冗余和非工作冗余。工作冗余是指冗余部分与工作部分同时工作，一旦工作部分出现故障则自动（或人工）切除故障部分，而其余部分继续工作。非工作冗余是指冗余部分一般不工作，处于等待状态。

由冗余资源组成的系统称为冗余系统，冗余资源的管理技术称为冗余技术。对于西门子自动化系统冗余技术而言，它主要分硬冗余和软冗余。西门子自动化系统的硬冗余是针对 S7-400H 系统的，其 CPU 自身具有冗余功能，由 CPU 硬件进行冗余运算，检测系统故障，主备 CPU 中的数据和事件保证完全一致，用于对主备系统切换时间有严格要求的场合，但成本较高。而西门子自动化系统的软冗余是指 S7-300/400 系统通过 MPI、PROFIBUS、Ethernet 等方式进行冗余，需有冗余软件包的支持，它是 SIEMENS 实现冗余功能的一种低成本的解决方案，但主备系统切换过程中产生的报警事件有可能丢失，因此它主要用于对主备系统切换时间要求不高的控制系统中。主备系统的切换时间为故障诊断检测时间、同步数据传输时间、DP 从

站切换时间之和，硬冗余主备系统切换时间为 200～300 微秒，软冗余主备系统切换时间为 300～600 毫秒甚至更长时间，受 CPU 型号及同步数据量的影响较大。

5.2 西门子 S7-300 软冗余系统的研究

5.2.1 S7-300 软冗余系统组成

为组建 S7-300 软冗余系统，需具备：STEP 7 编程软件、软冗余软件包、2 块 S7-300 CPU、2 块电源、3 条通信链路（主系统与从站之间的 PROFIBUS 通信链路、备用系统与从站之间的 PROFIBUS 通信链路、主系统与备用系统之间的 MPI 或 PROFIBUS 或 Ethernet 数据同步通信链路），若干个 ET200M 从站，每个从站包括 1 块电源和 2 个 IM153-2 接口模块（专用于冗余系统，每个模块提供 1 个 PROFIBUS 接口）。此外，还需编程计算机、下载适配器、PROFIBUS 或 Ethernet 连接线等[48][49]。

组建的 S7-300 软冗余系统结构图如图 5.2.1.1 所示。

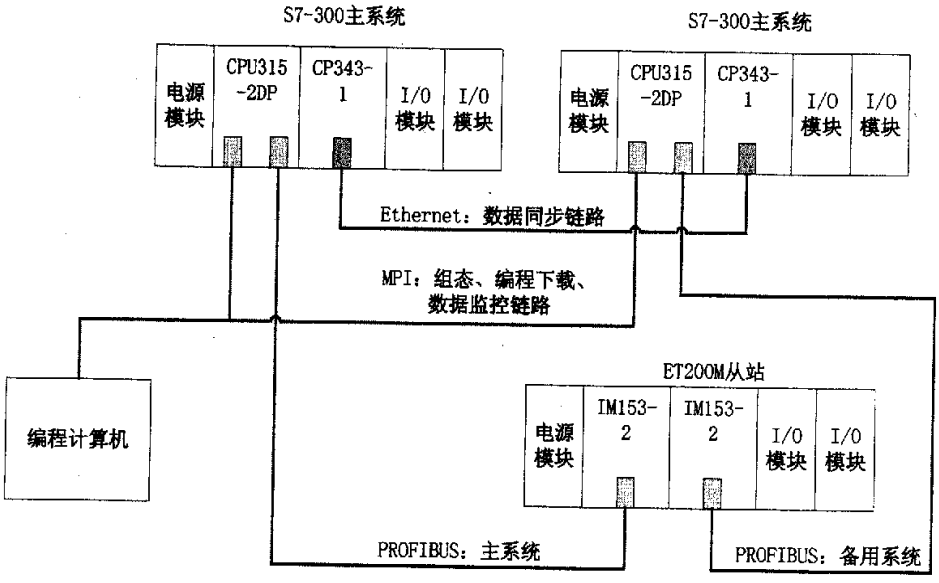


图 5.2.1.1 S7-300 软冗余系统结构图

该 S7-300 软冗余系统能实现主机架电源和背板总线的冗余、CPU 的冗余，PROFIBUS 现场总线的冗余以及 ET200M 从站接口模块 IM153-2 的冗余。当主系统中的任何一个模块出错，控制任务将会自动切换到备用系统中执行。即使系统没有发生故障，也可通过设定控制字手动切换主备系统。通常手动切换方式用于控制系统的软硬件调整、更换等场合。

S7-300 系列中除 CPU 314C-2DP、CPU 313C-2DP 以外，只有 315-2DP 型号以上的 PLC 才支持软冗余功能；此外，主系统与备用系统的 CPU 型号可以不同，如主备系统分别为 S7-400 CPU 和 S7-300 CPU。

5.2.2 S7-300 软冗余系统工作原理

在软冗余系统进行工作时，主备控制系统（处理器、通信链路、I/O 模块）独立运行，由主系统的 CPU 掌管对 ET200M 从站的 I/O 模块的控制权。主备系统中的 PLC 程序由非冗余（Non-Duplicated）用户程序段和冗余（Redundant Backup）用户程序段组成，主系统的 CPU 执行全部的用户程序，备用系统的 CPU 只执行非冗余用户程序段。运行过程如图 5.2.2.1 所示。

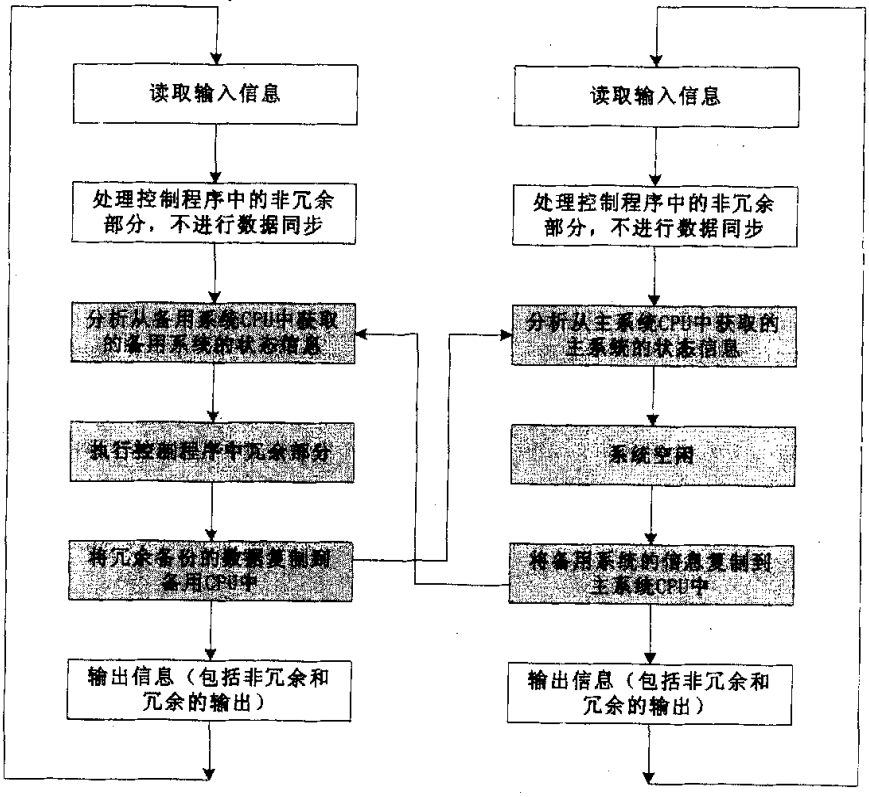


图 5.2.2.1 主备系统运行过程图

主备系统数据同步所需要的时间取决于同步数据量的大小和同步所采用的网络方式，Ethernet 网方式最快，PROFIBUS 方式适中，MPI 方式周期最长。

5.2.3 S7-300 软冗余系统组态与编程

在组态 S7-300 软冗余系统时，需注意：

（1）建立主系统（Master）站点和备用系统（Reserve）站点时，需创建相互独立的 PROFIBUS 网络：Master 和 Reserve，即分别创建主系统与从站通信链路和备用系统与从站通信链路，并将 PROFIBUS 地址设为相同。

（2）插入以太网模块 CP343-1 时，需将主备系统的 IP 地址设置在同一网段中（如 192.168.0.1 和 192.168.0.2），子网掩码为 255.255.255.0。否则无法进行数据同步。

（3）插入ET200M从站时，需将PROFIBUS地址也设置成相同。

（4）最后，需要在STEP 7的网络组态窗口NetPro中为数据同步链路建立连接。选中主系统CPU，建立新连接，将连接类型设置为基于以太网的连接："ISO-on-TCP connection"（若用CP342-5模块进行主备系统间的基于PROFIBUS的数据同步，则需创建"FDL connection"），并激活（Active）该链接。此时再查看Reserve站点，可看到激活状态为"No"。至此，该Master站设置为主系统了。网络组态图如图5.2.3.1所示。

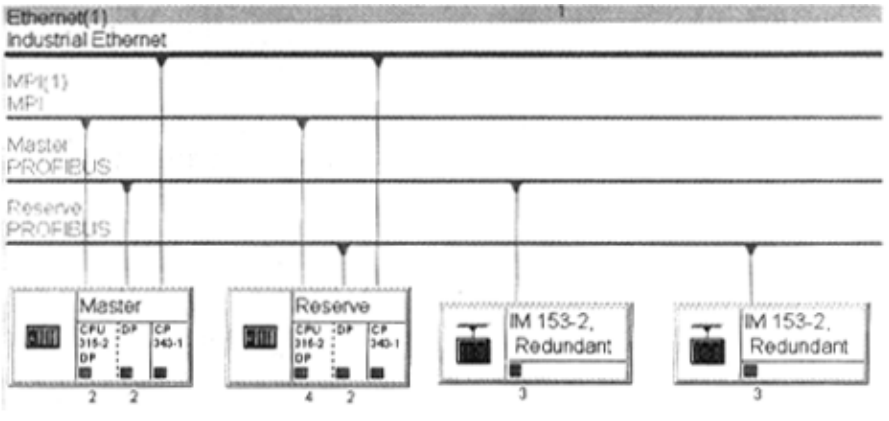


图5.2.3.1 S7-300软冗余系统网络组态图

在对S7-300软冗余系统编程时，需注意：

（1）需在主系统中插入OB1（主循环程序块）、OB35（定时中断组织块）、OB100（暖启动调用程序块）、OB80（在主系统与备用系统切换时间超时时，调用该块）、OB82（DP-Slave ET200站上的IM153-2模块出错报警，调用该功能块）、OB83（DP从站的接口模块与主站链接断开或链接重新建立时调用该块）、OB85（程序运行出错或DP从站连接失败调用该块）、OB86（主从站通信出错调用该块）、OB87（通信失败调用该块）、OB122（外围设备访问出错调用该块）、OB121等组织块，并对其中的OB100、OB35、OB86进行编程。

（2）一般在OB100暖启动块中进行软冗余的初始化操作，将非冗余程序段编写在主循环OB1中，而将冗余程序段编写在中断组织块OB35中。

（3）安装软冗余软件包后，会在STEP 7编程环境中出现新的函数库。其中SWR_XSEND_300和SWR_AGSEND_300是供S7-300系统使用的软冗余函数库。前者用于主备系统间通过MPI通信方式进行数据同步，后者适用于主备系统间通过PROFIBUS或Ethernet进行数据同步。SWR_AGSEND_300提供了FC100、FB101、FC102、FC104等功能块。FC100（SWR_START）用于初始化程序块，定义系统运行的参数；FB101（SWR_ZYK）是循环调用的数据同步功能块，将主系统中的冗余数据复制到备用系统中；FC102（SWR_DIAG）是诊断功能块，在OB86中调用，将得到的诊断数据

提供给 FB101 使用；

（4）通过 FB101 可得到状态字（含义见表 5.2.3.1）和控制字（含义见 5.2.3.2），从而可知系统当前状态。也可通过改变控制字，手动切换主备系统。

表 5.2.3.1 状态字含义说明

位 号		含 义
状态字低 8 位	0	1：本站为主系统
	1	1：本站为备用系统
	2	1：IDA，本站是 A 子站
	3	1：IDB，本站是 B 子站
	4	0：冗余功能激活；1：取消冗余功能
	5	0：冗余的同步连接正常；1：冗余的同步连接失败
	6	（无意义）
	7	1：运行状态
状态字高 8 位	0、1	（无意义）
	2	1：正在进行主备系统切换
	3	（无意义）
	4	1：主备系统切换过程中，通信忙
	5	1：与任何 DP 从站通信失败
	6	1：与部分 DP 从站通信失败
	7	1：与所有 DP 从站通信正常

表 5.2.3.2 控制字含义说明

位 号		含 义
控制字低 8 位	0	1：取消主备系统切换功能
	1	1：激活主备系统的切换
	2、3	（无意义）
	4	保留位，无须改变
	5～7	（无意义）
控制字高 8 位	0	1：手动激活主备系统的切换过程
	1～7	（无意义）

（6）在 OB35 中编写冗余程序时，需按照如图 5.2.3.2 所示流程进行。

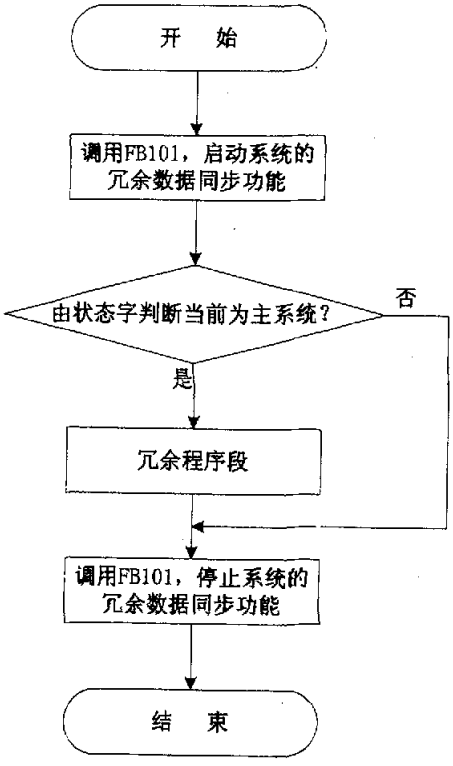


图 5.2.3.2 冗余程序流程图

5.3 小结

冗余技术利用外加的资源，保证控制系统的可靠性。S7-300 系统软冗余技术是 SIMATIC 低成本的冗余解决方案，作者研究了其系统组成、冗余原理，总结了组态（基于 Ethernet 方式的数据同步）及编程需注意之处。

在自动控制系统中虽然可采用冗余技术提高系统的可靠性，但也不可一味追求冗余度大、冗余范围广，必须符合实际应用的需求，从实用性、有效性和成本等方面综合考虑，设计出性价比最高的满足实际应用要求的冗余系统。

结 束 语

作者以某高校西门子工业控制网络实验室建设为背景，主要研究了其中的通信技术、OPC 应用程序标准接口技术、基于 PC 的自动化产品 WinAC 系统和软冗余技术。MPI 通信主要用于编程设备的组态、编程，也可用于少数 CPU 之间传递少量数据，它的三种通信方式：全局数据包 MPI 通信、无组态连接的 MPI 通信、组态连接的 MPI 通信都有各自的适用条件和组态、编程方法，文中进行了总结和比较。PROFIBUS 现场总线以其数字化、开放性和互操作性等特点，在现场总线领域占据重要位置。基于 PROFIBUS-DP 协议的 FDL 通信保证了高等级的传输安全性，而基于 PROFIBUS-DP 的 DX 通信可以提高自动化系统中从站间的通信效率。PROFInet 工业以太网的兴起预示了现场总线从管理级向现场级延伸的趋势，现场总线趋于统一化，这是当今工控界普遍关心的热点问题，相信在短期内二者仍会并存，互相融合，发挥各自的优势。

OPC 接口技术保证了工业控制系统应用程序通信接口的标准化。该接口技术不仅能够应用于单台计算机，而且可以支持网络上分布式应用程序之间的通信，以及不同平台上应用程序之间的通信。它相当于为不同设备制造商的设备提供了公共的驱动程序接口，方便了自动化系统的集成，增强了系统的开放性与灵活性。

WinAC 是西门子公司基于 PC 的自动化解决方案的典型代表，它充分利用了 PC 机丰富的硬件资源和软件接口，将控制、监控、数据处理集成在一起，可实现较为复杂的算法，完成特殊控制任务，如运动控制、视觉系统，降低了系统成本。基于 PC 的控制系统的出现并未将传统硬 PLC 推向末路，因为后者可完成大部分控制任务，并以其高可靠性赢得人们的青睐。在国内，大多数行业仍倾向于选择传统的硬 PLC 完成控制任务。

为了提高控制系统的可靠性，冗余技术得到了应用。S7-300 系统的软冗余技术是西门子实现冗余功能的一种低成本的解决方案，适合对主备系统切换时间没有严格要求的场合。

作者对上述技术进行了研究、探讨和应用，并设计了若干实例加以验证，给出了相关设计方法和注意点。

西门子工业控制网络技术的内涵博大精深，作者仅选取了其中一部分进行了研究，另外还有许多技术如控制网络扩展技术、诊断技术、无线通信技术、光纤网通信技术等，有待继续研究和学习。

致　谢

本文是在导师姜建芳教授的悉心指导下完成的。导师严谨笃实一丝不苟的工作作风、循循善诱诲人不倦的指导风格、谆谆教导严格要求的育人方式，使我在硕士研究生学习中，不论是思维方式还是实际的动手能力都取得了很大的进步。他不仅教会我新知识，还教我做人，在生活方面给予了我父母般的关心和帮助。他给了我许多次锻炼的机会，不仅从中学到了专业知识，同时也锤炼了我的意志品质，为我今后走向社会培养了良好的修养，打下了较好的基础。在此谨向他表示最衷心的感谢！

在完成项目和论文期间，还得到了教研室其他同学的大力协助，在此一并表示感谢！

陈　建

2005 年 6 月

参考文献

1 PROFIBUS-DP. PROFIBUS International, 1997

2 PROFIBUS 技术和应用. PROFIBUS International, 2002

3 余华军. 现场总线技术及其发展. 浙江电力. 2004(3)

4 SIMATIC NET Profibus Networks. SIEMENS AG, 2003

5 徐世许. 可编程序控制器原理、应用、网络. 中国科技大学出版社，2000

6 PROFIBUS 技术标准. PROFIBUS Professional Organization, 2001

7 张海淑，傅仲述. 现场总线技术及其应用. 福建电脑. 2004(7)

8 殷华文、刘黎明、刘万里. 工业控制网络设计技术. 自动化仪表，2002

9 宋国强. 现场总线纵横谈. 上海电机技术高等专科学校学报. 2004(2)

10 O' Connel L. Getting ethernet ready for the factory floor[J]. 2003(2)

11 仲兆峰，许星，程良伦. 基于 PROFIBUS 总线技术的工业网络的设计与实现. 微机算计信息. 2003(11)

12 现场总线（PROFIBUS）技术应用论文集（第一辑）. 中国机电一体化技术应用协会现场总线（PROFIBUS）专业委员会出版

13 现场总线（PROFIBUS）技术应用论文集（第二辑）. 中国机电一体化技术应用协会现场总线（PROFIBUS）专业委员会出版

14 袁任光. 可编程序控制器（PC）应用技术与实例. 华南理工大学出版社，1997

15 姜建方，向峥嵘. 可编程序控制器应用技术. 南京理工大学自动化系，2002

16 SIMATIC S7-200 可编程序控制器系统手册. SIEMENS AG，2000

17 Configuring Hardware and Communications STEP 7 V5.0. SIEMENS AG，1999

18 郭宗仁. 可编程序控制器及其通信网络技术. 人民邮电出版社，1999

19 STEP 7 V5.0 User Manual. SIEMENS AG，1999

20 门槛创作室. Visual Basic 6.0 实例教程. 电子工业出版社，1999

21 崔坚，李佳. 西门子工业网络通信指南. 机械工业出版社，2005

22 王珍熙. 可靠性冗余及容错技术. 航空工业出版社，1991

23 邬宽明. 现场总线技术应用选编. 北京航空航天大学出版社，2003

24 PROFIBUS 总线协议. PROFIBUS International, 1997

25 Profibus Technical Description. PNO，1999

26 西门子（中国）有限公司. 走进现场总线 PROFIBUS 的殿堂. 加工技艺. 2004(6)

27 郭宗仁，吴亦锋，郭永. 可编程序控制器应用系统设计及通信网络技术. 人民邮电出版社，2002

28 侯维岩，张海峰，费敏锐. 现场总线 PROFIBUS 系统的实时性能分析. 电子测量与仪器学报. 2004(2)

29 Introduction to Profibus on Industrial PC. SIEMENS AG，2003

30 邱公伟. 可编程控制器网络通信及应用. 清华大学出版社，2000

31 刘晓光，陈伟彬，吴勤勤. OPC 技术在工业自动化中的应用. 电气时代. 2003(7)

32 何海江，何海平，黄锁彬. 基于 OPC 协议的化工 DCS 网络. 化工自动化及仪表. 2003(6)：33-35

33 李南，薛孝存，王大海，利铭. 浅谈 OPC 技术. 中国仪器仪表. 2003(1)

34 陈帅，杨洪波. 用于过程控制的对象连接和嵌入技术综述. 计算机技术与应用. 2003(2)

35 OPC 协议规范. OPC 中国. 2003

36 钟霖田. OPC一全开放控制系统的核心构件. 自动化博览. 2002(2)

37 邹云涛，吴重光. OPC DA 客户端的三种实现方式. 中国自动化控制网. 2004(1)

38 西门子（中国）有限公司. SIMATIC WinAC一基于 PC 的自动化系统. 2000(9)

39 西门子（中国）有限公司. SIMATIC 基于 PC 的自动化系统一WinAC. 自动化与仪器仪表. 2003(1)

40 刘云，周海涛. 基于 PC 的自动化控制. 微机算计信息. 2002(9)

41 深入浅出 WinAC. SIEMENS AG，2005

42 Computing OPC Server Interface. SIEMENS AG, 2004

43 SIMATIC Computing User Manual. SIEMENS AG, 2000

44 SIMATIC Windows Logic Controller User Manual. SIEMENS AG, 2000

45 牛晓玮. SIMATC 基于 PC 的自动化. SIEMENS AG, 2004

46 SIMATIC 视窗自动化中心 WinAC Basis 概述. SIEMENS AG, 2001

47 SIMATC 基于 PC 的自动化. SIEMENS AG, 2004

48 PLC 系统软件冗余的说明与实现. SIEMENS AG, 2004

49 Software Redundancy for SIMATIC S7-300 and S7-400. SIEMENS AG, 2003

50 唐勇奇，赵葵银. PC-PLC 组成的电梯群控系统. 应用科技. 2001(1)

51 吴宗泽，武自芳. 基于 PROFIBUS 的多目标规划电梯群控算法. 2003(3)

52 弓箭，刘强，刘剑. 人工智能在电梯群控系统中的应用. 沈阳建筑工程学院学报. 2002(4)

53 李秋明，顾德英，汪晋宽. 基于工业三层网络的电梯群控系统. 仪器仪表学报. 2003(4)

54 Protool 基于 Windows 系统的组态. SIEMENS AG，2000

55 SIMATIC HMI 基于 Windows 的系统的通信用户手册. SIEMENS AG，2000

附 录

研究生期间公开发表的论文：

1 ActiveX 在 WinCC 归档数据复杂查询中的研究与实现. 工业控制计算机. 2005(5).

西门子工业控制网络技术研究与应用

作者：陈建
学位授予单位：南京理工大学

参考文献(56条)

1. 参考文献

2. PROFIBUS-DP. PROFIBUS International 1997

3. PROFIBUS技术和应用. PROFIBUS Internati onal 2002

4. 余华军 现场总线技术及其发展[期刊论文]-浙江电力 2004(3)

5. SIMATIC NET Profibus Networks 2003

6. 徐世许 可编程序控制器原理、应用、网络 2000

7. PROFIBUS技术标准 2001

8. 张海淑. 傅仲逑 现场总线技术及其应用 2004(07)

9. 殷华文. 刘黎明. 刘万里 工业控制网络设计技术[期刊论文]-自动化仪表 2002(11)

10. 宋国强 现场总线纵横谈[期刊论文]-上海电机技术高等专科学校学报 2004(2)

11. O’Connel L Gerting ethernet ready for the factory floor 2003(02)

12. 仲兆峰. 许星. 程良伦 基于PROFIBUS总线技术的工业网络的设计与实现[期刊论文]-微计算机信息(测控仪表自动化) 2003(11)

13. 现场总线(PROFIBUS)技术应用论文集

14. 现场总线(PROFIBUS)技术应用论文集

15. 袁任光 可编程序控制器(PC)应用技术与实例 1997

16. 姜建方. 向峥嵘 可编程序控制器应用技术 2002

17. 16SIMATIC S7-200可编程序控制器系统手册 2000

18. Configuring Hardware and Communications STEP 7 V5.0 1999

19. 郭宗仁 可编程序控制器及其通信网络技术 1999

20. STEP 7 V5.0 User Manual 1999

21. 门槛创作室 Visual Basic 6.0实例教程 1999

22. 崔坚. 李佳 西门子工业网络通信指南 2005

23. 王珍熙 可靠性冗余及容错技术 1991

24. 邬宽明 现场总线技术应用选编 2003

25. PROFIBUS总线协议. PROFIBUS International 1997

26. Profibus Technical Description 1999

27. 西门子(中国)有限公司 走进现场总线PROFIBUS的殿堂 2004(06)

28. 郭宗仁. 吴亦锋. 郭永 可编程序控制器应用系统设计及通信网络技术 2002

29. 侯维岩. 张海峰. 费敏锐 现场总线PROFIBUS系统的实时性能分析[期刊论文]-电子测量与仪器学报 2004(2)

30. Introduction to Profibus on Industrial PC 2003

31. 邱公伟 可编程控制器网络通信及应用 2000

32. 刘晓光. 陈伟彬. 吴勤勤 OPC技术在工业自动化中的应用[期刊论文]-电气时代 2003(7)

33. 何海江. 何海平. 黄锁彬 基于OPC协议的化工DCS网络[期刊论文]-化工自动化及仪表 2003(6)

34. 李南. 薛孝存. 王大海. 利铭 浅谈OPC技术[期刊论文]-中国仪器仪表 2003(1)

35. 陈帅. 杨洪波 用于过程控制的对象连接和嵌入技术综述 2003(02)

36. OPC协议规范 2003

37. 钟霖田 OPC-全开放控制系统的核心构件[期刊论文]-自动化博览 2002(2)

38. 邹云涛. 吴重光 OPCDA客户端的三种实现方式 2004

39. 西门子(中国)有限公司 SIMATIC WinAC--基于PC的自动化系统 2000(09)

40. 西门子(中国)有限公司 SIMATIC基于PC的自动化系统--winAC 2003(01)

41. 刘云. 周海涛 基于PC的自动化控制[期刊论文]-微计算机信息(测控仪表自动化) 2002(9)

42. 深入浅出WinAC 2005

43. Computing OPC Server Interface 2004

44. SIMATIC Computing User Manual 2000

45. SIMATIC Windows Logic Controller User Manual 2000

46. 牛晓玮 SIMATC基于PC的自动化 2004

47. SIMATIC视窗自动化中心winAC Basis概述 2001

48. SIMATC基于PC的自动化 2004

49. PLC系统软件冗余的说明与实现 2004

50. Software Redundancy for SIMATIC S7-300 and S7-400 2003

51. 唐勇奇. 赵葵银 PC-PLC组成的电梯群控系统[期刊论文]-应用科技 2001(1)

52. 吴宗泽. 武自芳 基于PROFIBUS的多目标规划电梯群控算法 2003(03)

53. 弓箭. 刘强. 刘剑 人工智能在电梯群控系统中的应用[期刊论文]-沈阳建筑工程学院学报(自然科学版) 2002(4)

54. 李秋明. 顾德英. 汪晋宽 基于工业三层网络的电梯群控系统 2003(04)

55. Protool基于Windows系统的组态 2000

56. SIMATIC HMI基于Windows的系统的通信用户手册 2000

相似文献(10条)

1. 学位论文 李亚男 现场总线关键技术的研究及实现 2002

该文对PROFIBUS通信协议作了深入研究,尤其侧重于对PROFIBUS-DP从站的研究.论文中介绍了PROFIBUS的基本特性、协议结构、总线存取协议,详细阐述了PROFIBUS-DP的数据链路层（FDL）协议、报文格式、服务类型及传输过程,透彻分析了DP从站的功能、态机制及它与主站间通信的详尽过程.对PROFIBUS-DP系统通信模型作了总结.该文在研究PROFIBUS-DP标准的基础上,提出了DP从站的实现方案,并完成了产品开发,研制了智能从站及简单从站,同时我们还设计了光模块,以使PROFIBUS系统能用光缆来传输信号,增加其传输距离.

2. 期刊论文 陈景文. 王红艳 Profibus总线通信协议在造纸中的应用 -电气应用2005,24(4)

介绍了Profibus总线通信协议并列举了其在造纸机传动设计上的一个应用实例.

3. 学位论文 梁传波 PROFIBUS DP现场总线多功能从站设计 2006

现场总线是一种应用于生产现场，在现场设备之间、现场设备与控制装置之间实现双向、串行、多节点数字通信的技术。PROFIBUS是当今最为流行的现场总线之一，其中PROFIBUS DP作为一种优化的高速通信连接，应用又最为广泛。但时至今日，现场总线领域也没有形成一套统一的标准，自动化孤岛依然存在，在这样的背景下，每种总线都缺乏一定的通用性。

本课题旨在为PROFIBUS DP这一特定总线，设计一款通用的多功能从站接口，从而使普通的设备可方便的挂接到总线上。本文首先对PROFIBUS DP的总线通信原理进行了分析，然后以此为依据，深入探讨了从站的软硬件设计，其中重点阐述了从站在实现通信协议基础之上的多功能扩展，并对每种功能的实现加以详述。多功能化的扩展使从站可以提供多种接口，用于挂接包括模拟的、数字的、并行的以及串行的各类通信设备。最后，为了完善从站的多功能化，本文又对配套的上位机软件设计以及最终通信系统的搭建依次做了论述。

最后对课题的研究工作进行了总结与展望。

4. 期刊论文 方彦军. 李京丽. 陈梅城 PROFIBUS-DP现场总线智能从站通信协议研究 -仪表技术与传感器2004,""(12)

从PROFIBUS-DP数据通信网络的总线配置出发,介绍了PROFIBUS-DP通信网络的构建方法以及DP主站与DP从站的工作机制、主要工作任务和数据交换过程.在此基础上详细说明了PROFIBUS-DP协议的结构,包括数据传输报文、安全机制和可用的传输服务.最后以协议芯片SPC3为核心,提出了一种PROFIBUS-DP协议在从站模块中的程序实现方法,同时对其程序的工作流程作了简单介绍.

5.学位论文 赵青 列控系统中STM的PROFIBUS接口研究设计 2007

中国铁路参照ERTMS/ETCS中对列车控制系统的发展分级，制定了我国的CTCS的发展分级。ETCS系统中规定了STM接口的多层协议，CTCS对STM的接口几乎没有规定。本文从适应设备引进，与国际接轨等角度出发，探讨了作为STM底层的PROFIBIJS接口研究设计，具有理论和现实意义。论文主要包括以下几个方面：

1、首先介绍了STM的定义、用途及ETCS对STM的PROFIBUS接口的要求。并且介绍了PROFIBUS现场总线的特点、优点和相关标准。

2、重点研究了STM的PROFIBUS接口的硬件电路和软件设计。其中硬件是以DSP为控制器基于SPC3进行研究开发的，这样能更加保证数据的高速、高可靠性传输。硬件设计主要包括：基本DSP电路的设计；供电电源的设计；DSP复位电路的设计；SPC3接口电路设计；电平转换模块的设计；SPC3与DSP的连接。软件部分设计主要是依靠PROFIBUS-DP通信协议和STM接口通信协议及报文格式要求进行。软件设计主要包括：通信关系的建立，数据处理和GSD文件的编写。

3、最后利用Siemens公司的PACKAGE4进行组网实验。介绍了主站接口模块(IM180+IM181)，以及组网实验的具体步骤和操作方式，建立了从站和主站之间的简单通讯，实现了设计要求。

6.期刊论文 付晓梅.戴居丰.文炜.马晓红 MC68340用于Profibus现场总线通信协议管理 -工业控制计算机2001,""(2)

本文对Profibus现场总线的通信协议管理进行了讨论,通过提出MC68340仿真实现的方案,给出了实现Profibus协议第二层主要服务的基本框架.

7.学位论文 杨家强 基于Profibus-PA现场总线接口技术的研究与开发 2003

该课题来源于机械工业部仪表综合技术经济研究所与PROFIBUS现场总线基金会的合作开发项目:PROFIBUS_PA接口技术的研究与开发,是该课题的一个子课题.该课题的主要任务是研究PROFIBUS_PA总线通信协议,设计符合PROFIBUS_PA通信协议的智能接口模块,设计无刷无位置传感器电机变频控制系统,将电机变频控制系统与PROFIBUS_PA总线相连,实现总线对电机转速的控制.PROFIBUS现场总线是现今在工业过程控制领域用的最为广泛的现场总线,应用领域包括制造业自动化,流程工业自动化,楼宇自动化,交通电力甚至食品,化工等领域.在国际上,已经有上百家企业生产品种繁多PROFIBUS总线产品,在国内,用户也非常欢迎PROFIBUS总线产品,在国内也有一些企业开发PROFIBUS_DP接口产品,但还没有一家企业自己能够开发并提供PROFIBUS_PA总线产品,所以现在国内市场上的PROFIBUS_PA总线接口产品都是由国外引进的,价格昂贵,因此该课题的研究是及时填补了一种有极大市场潜力的研究领域,对自动化控制领域技术进步和缩小与国外技术水平的差距,具有重要意义.

8.期刊论文 何波丽.李胜旺.HE Bo-li.LI Sheng-wang PROFIBUS-DP现场总线通信协议 -河北工业科技2009,26(5)

以开放式系统互联模型ISO/OSI为参考,描述了PROFIBUS-DP现场总线通信协议的结构,包括物理层的数据传输介质与数据传输格式,数据链路层的数据报文与数据传输服务调用方法及可用的传输服务.介绍了PROFIBUS-DP通信协议芯片SPC3的结构特点和功能,给出了SPC3与单片机AT89S52的接口电路图和相关的软件流程图.

9.学位论文 周益明 PROFIBUS-DP现场总线通信研究及智能从站设计 2005

现场总线综合了数字通信技术、计算机技术、自动控制技术、网络技术和智能仪表技术等多种技术手段,构成了一种全分散、全数字、智能、双向、互连、多变量、多接点的通信与控制系统,成为自动控制发展的趋势.在现有的各种现场总线标准中,PROFIBUS总线是一种比较流行的现场总线标准,用于设备级控制系统与分散式I/O通信的PROFIBUS-DP是市场占有率绝对领先的总线技术.目前,我国对于PROFIBUS-DP的应用和研究主要以西门子等公司的成套设备为主,而自主研究开发通信接口的却比较少.如何为仪表或电气设备开发PROFIBUS-DP通信接口,使国产设备能连接到PROFIBUS总线中,以推动我国仪表业的智能化进程和现场总线在我国的应用就显得尤为重要.本文正是针对现场总线在我国的应用和发展现状,在研究PROFIBUS-DP现场总线基本理论(主要包括系统组成、协议结构、数据存取机制、通信原理)的基础上,提出了PROFIBUS-DP智能从站接口的软硬件设计和实现方法,利用PROFIBUS-DP协议芯片SPC3和51单片机开发出具有PROFIBUS-DP接口的数字量输入输出智能化从站接口模块,接着由CP5611作为主站,结合开发的从站接口模块组成单主站单从站的PROFIBUS-DP现场总线最小系统,对开发的从站接口模块进行了实验验证.最后本文对课题的研究工作进行了总结,并对PROFIBUS-DP智能从站接口开发和系统集成方面提出了进一步的研究方向和方法.

10.期刊论文 杜永.张赤斌.DU Yong.ZHANG Chi-bin 互换总线协议的PROFIBUS通信 -金陵科技学院学报2009,25(1)

总线桥是指通过一个自行定义的双向并行通信协议,获得总线间的高速数据通信能力.同时,间接实现多种总线标准的协议转换.重点介绍RS232/485接口的现场设备连到PROFIBUS网络的通信协议及其核心硬件结构.