摘 要

本文主要的工作是通过一个实际的项目，进行了基于西门子公司 SIMATIC SINEC 工业现场通信网络的研究与设计。作者采用目前日益流行的现场总线技术，构建了新一代 FCS（现场总线控制系统）的雏形，实现了现场设备和操作站之间的数据交换，为企业建设 CIMS 乃至企业全面的信息化打下了坚实的基础。

在项目开发过程中，全部的通信程序都是在 STEP5 语言环境下编制完成的，并且通过西门子公司功能强大的 WinCC 软件包对网络进行了组态，保证了整个系统的可靠性。本文提供了一种工业现场通信组网的方案，在提高国内企业生产力水平和与国际接轨程度方面，具有一定推广的价值。

关键词：现场总线，FCS，PROFIBUS，SINEC-H1，SINEC-L2

Abstract

By a practical engineering, this paper is about Research & Design job of Industrial Field LANs based on the SIAMTIC SINEC, SIEMENS Corp. The author constructed a rudiment of FCS, which was the abbreviation for **fieldbus control system**, by using Fieldbus Technology, and accomplished the data communication between operating stations and field equipments. This kind of job is the base of CIMS and enterprise information networks.

In the engineering, all of programs were written on the SIEMENS STEP5 platform, and network configurations were done by WinCC software packet, which guaranteed the reliability of system. A scheme constructing industrial field communication network was provided here, which should be extended in order to promote the productivity of domestic enterprises.

Key Words: Fieldbus, FCS, PROFIBUS, SINEC-H1, SINEC-L2

1 绪论

1.1 工业通信系统的发展

七十年代以前，工业控制通信系统中采用模拟量对数据及控制信号进行转换、传递，其精度差、受干扰信号影响大，因而整个系统的控制效果及稳定性都很差。七十年代末，随着大规模集成电路的出现，微处理器技术得到很大发展。微处理器功能强、体积小、可靠性高、通过适当的接口电路用于控制系统，控制效果得到提高；但是尽管如此，还是属于集中式控制系统。随着过程控制技术、自动化仪表技术和计算机网络技术的成熟和发展，控制领域又发生了一次技术变革。这次变革使传统的控制系统无论在结构上还是在性能上都发生了巨大的飞跃，这次变革的基础就是现场总线技术的产生。

现场总线是连接现场智能设备和自动化控制设备的双向串行、数字式、多节点通信网络，它也被称为现场底层设备控制网络。80 年代以来，各种现场总线技术开始出现，人们要求对传统的模拟仪表和控制系统变革的呼声也越来越高，从而使现场总线成为一次世界性的技术变革浪潮。

由现场总线构成的工业通信系统称为现场总线控制系统（FCS，Fieldbus Control System）。FCS 系统针对现存的 DCS（集散控制系统）的某些不足，改进控制系统的结构，提高其性能和通用性。在开放性、控制分散及通信性能等方面优于传统 DCS。

1.2 现场总线控制系统（FCS）的结构与特点

- 结构

随着现场总线技术的出现和成熟，促使了控制系统由集散控制系统（DCS）向现场总线控制系统（FCS）的过渡。在一般的 FCS 系统中，遵循一定现场总线协议的现场仪表可以组成控制回路，使控制站的部分控制功能下移分散到各个现场仪表中。从而减轻了控制站负担，使得控制站可以专职于执行复杂的高层次的控制算法及通信任务。对于简单的控制应用，甚至可以把控制站取消，在控制站的位置代之以起连接现场总线作用的网桥和集线器，操作站直接与现场仪表相连，构成分布式控制系统。

- 特点

分布式的 FCS 系统比 DCS 系统更好地体现了“信息集中，控制分散”的思想。与传统的 DCS 相比，FCS 有其自身的特点。FCS 系统具有高度的分散性，它可以由现场设备组成自治的控制回路。现场仪表或设备具有高度的智能化与功能自主性，可完成控制的基本功能，并可以随时诊断设备的运行情况。另外，FCS 的结构比 DCS 简化。有的 FCS 系统省略了 DCS 中控制站这一层，操作站直接与现场仪表相连。这些使 FCS 的可靠性得到提高。

现场总线系统具有开放性。系统对相关标准具有一致性、公开性，强调对标准的共识与遵从。通信协议一致公开，各不同厂家的设备之间可实现信息交

换，通过现场总线可构筑自动化领域的开放互连系统。系统的开放性决定了它具有互操作性和互用性。互操作性指互连设备间、系统间信息传送与沟通；而互用则意味着不同生产厂家的性能类似的设备可实现相互替换。作为工厂网络底层的现场总线还对现场环境有较强地适应性。它支持双绞线、同轴电缆、光缆、无线和电力线等，具有较强的抗干扰能力。

由于结构上的改变，FCS 比 DCS 更节约硬件设备。使用 FCS 可以减少大量的隔离器、端子柜、I/O 卡及 I/O 端口，这样就节省了 I/O 装置及装置室的空间；同时减少了大量电缆，可以极大地节省安装费用。与此同时，FCS 比 DCS 性能有所提高。由于免去了 D/A 与 A/D 变换，使仪表精度得到极大的提高；目前 FCS 可以从 DCS 的每秒调节 2~5 次增加到每秒调节 10~20 次，改善了调节性能。

由于现场总线的以上特点，特别是其系统结构的简化，使其从设计、安装、投运到正常生产运行及检修维护，都体现出优越性。它不仅节省了硬件数量与投资，节省了安装费用，而且系统的维护开销也大大地降低。现场总线控制系统不仅精确度与可靠性高，在方便使用和维护性方面，FCS 也比 DCS 有优势。FCS 使用统一的组态方式，安装、运行、维修简便；利用智能化现场仪表，使维修预报成为可能；由于系统具有互操作性和互用性，用户可以自由选择不同品牌的设备达到最佳的系统集成，在设备出现故障时，可以自由选择替换的设备，保障用户的高度系统集成主动权。

此外，它还具有设计简单，易于重构等特点。

1.3 课题来源及意义

随着国民经济和科技飞速发展以及我国加入WTO后信息交流的日益频繁，一个国家的企业信息化程度的高低，已经成为衡量发展水平的重要标志。在市场经济与信息社会中，网络对企业的综合竞争力发挥着越来越重要的作用。要把企业经营决策、计划、调度、过程优化、故障诊断、现场控制紧密联系在一起，进行综合信息处理，按市场需求，以尽可能低的资源、能量消耗，以最短的时间，开发并生产出新的产品供应市场，就必须将自动控制、办公自动化、经营管理、市场销售等各层次计算机互连成一个多层次网络，实现信息的沟通与数据共享，这便是企业信息化的概念。但是国内不少生产企业，技术还比较陈旧，生产力水平得不到充分发挥，难以面对日益激烈的市场竞争。

如何适应现代市场经济下各种行业的激烈竞争，抵御国外企业的冲击，已成为国内企业高度关注的问题。提高企业的综合实力，其中非常重要的一环就是提高企业的技术水平。

在上述背景下，本课题来源于盐城八菱化纤的工业通信网络。化纤生产线是一条连续化的生产线，工业流程比较长，工艺中需要测量、控制和保护的工艺参数多，因此数据传输量大。目前完成机械设备动作控制的主要装置是西门子（SIEMENS）公司的 S5 系列可编程控制器，现场通信任务由 SIMATIC SINEC

网络完成。

1.4 课题的主要任务

本文是针对盐城八菱化纤后纺车间的课题而进行的设计研究。通过对企业的调查研究，进行了分散式现场通信系统的设计研究开发，从技术上论述如何用 SINEC-H1 网、SIENC-L2 网实现和现场设备及操作站之间的数据通信。课题的主要工作为：

- 进行可编程控制器的通信程序的编制。
- 进行西门子 SINEC-H1 网总体框架设计。
- 进行西门子 SINEC-L2 网总体框架设计。
- 进行通信模板的组态。
- 进行基于 SIMATIC SINEC 网络的互连设计
- 为车间和工厂 CIMS 网的连接打下良好的基础。

2　系统总体结构分析与设计

化纤厂将原料制成符合客户要求的化纤产品分为两步：一是将原料粗加工成半成品；二是根据客户具体的品质要求将半成品进一步细加工。这两个步骤称为前纺和后纺，分别由前纺车间和后纺车间完成。由于前纺数据要求基本相同，工艺流程较少，所以结构相对简单。而本文的重点则放在较为复杂的后纺车间，讨论其网络结构及其通信的实现。

后纺车间的工艺流程见图 2.1 所示。

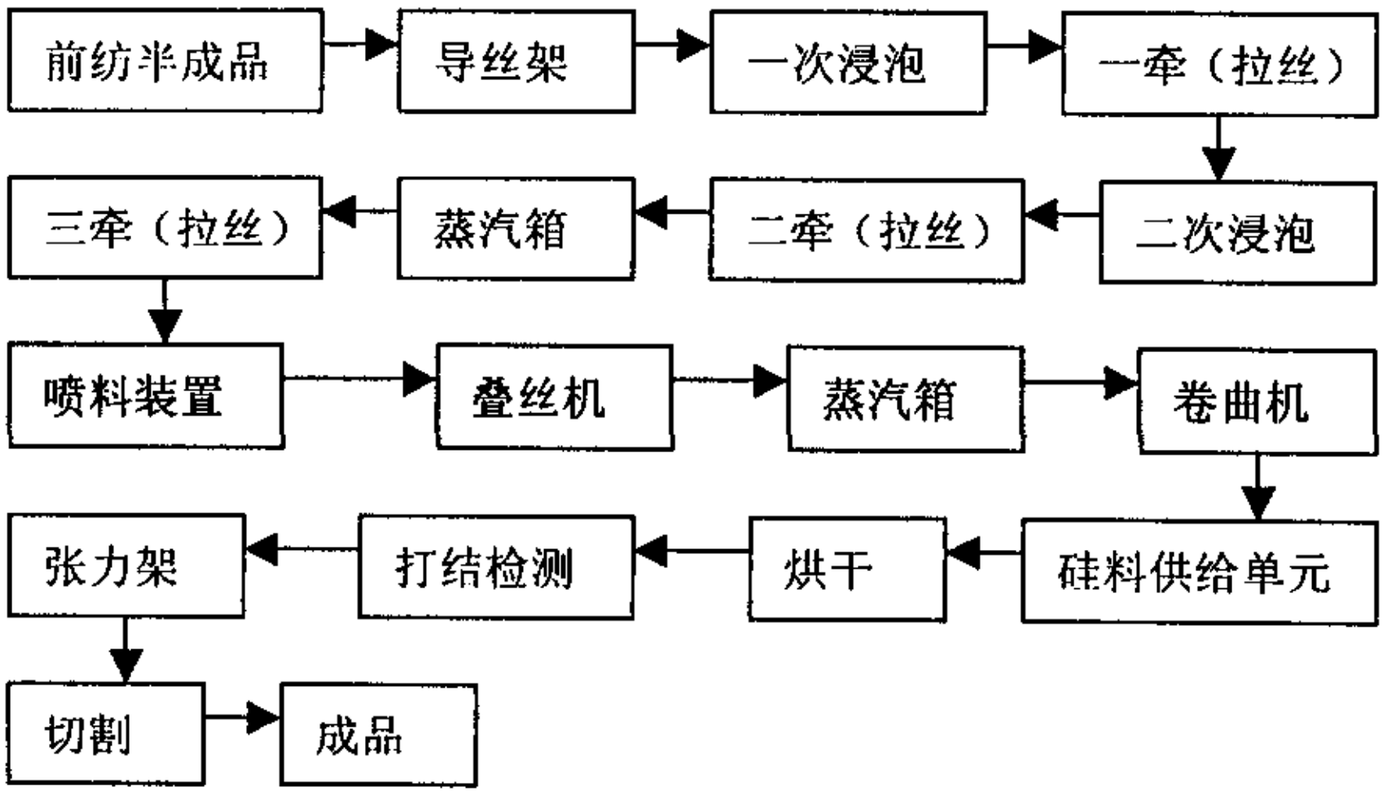


图 2.1　后纺的生产流程

后纺的生产工艺流程是进行本控制系统设计的基础和依据。下面结合生产工艺流程详细阐述系统的结构设计。

2.1 现场控制站的设计与功能实现

现场控制站主要完成对过程现场输入输出信号的处理并实现直接数字控制（DDC）功能。它是本系统的基础控制站，任何其它功能都是通过它而实现的。其主要功能有三个：

- 将各种现场发生的过程量（流量、压力、液位、温度、电流、电压、功率以及各种状态等）进行数字化，并将这些数字化后的过程量存在存储器中，形成一个与现场过程量一致的、能一一对应的、并按实际运行情况实时地改变和更新的现场过程量的实时映像；
- 将本站采集到的实时数据通过通信网络送到操作管理站，以便实现全系统范围内的监督和控制，同时现场控制站还可以接受由操作管理站下发的信息，以实现对现场的人工控制或对本站的参数设定；
- 在本站实现局部自动控制、回路的计算及闭环控制、人工控制等控制功

能，所采用的算法一般是经典的 PID 控制算法，也可以通过与操作管理站通信实现复杂的预测算法。

通过以上的分析，可以知道现场控制站本身实质上是一个基本的过程计算机控制系统。在本系统的设计中，现场控制站采用的是可编程控制器。

目前市场上可编程控制器产品种类众多，若按其发展的历史渊源及所受的地域影响来划分，大体可以分为三个流派，即美国产品、日本产品及欧洲产品。这其中西门子（SIEMENS）公司的产品颇具特色，它的 S5 系列产品不仅规格齐全，而且还提供品种众多的通信处理器模板及其配套的软件功能块，方便了对于通信系统的开发。鉴于此，系统采用西门子的 S5-135U 可编程控制器作为现场控制站，中央处理器选用 CPU928，并使用配套的 STEP5 语言环境编制用户通信程序。下面具体阐述设计思想与功能实现。

2.1.1　可编程控制器的工作原理

可编程控制器虽具有微机的许多特点，但它的工作方式却与微机有很大不同。微机一般采用等待命令的工作方式，如常见的键盘扫描方式或 I/O 扫描方式，有键按下或 I/O 动作，则转入相应的子程序，无键按下，则继续扫描。而可编程控制器则采用循环扫描工作方式。在可编程控制器中，用户程序按先后顺序存放。

CPU 从第一条指令开始执行程序，直至遇到结束符后又返回第一条。如此周而复始不断循环。每一个循环称为一个扫描周期。一个扫描周期大致可分为 I/O 刷新和执行指令两个阶段，如图 2.1.1.1 所示。

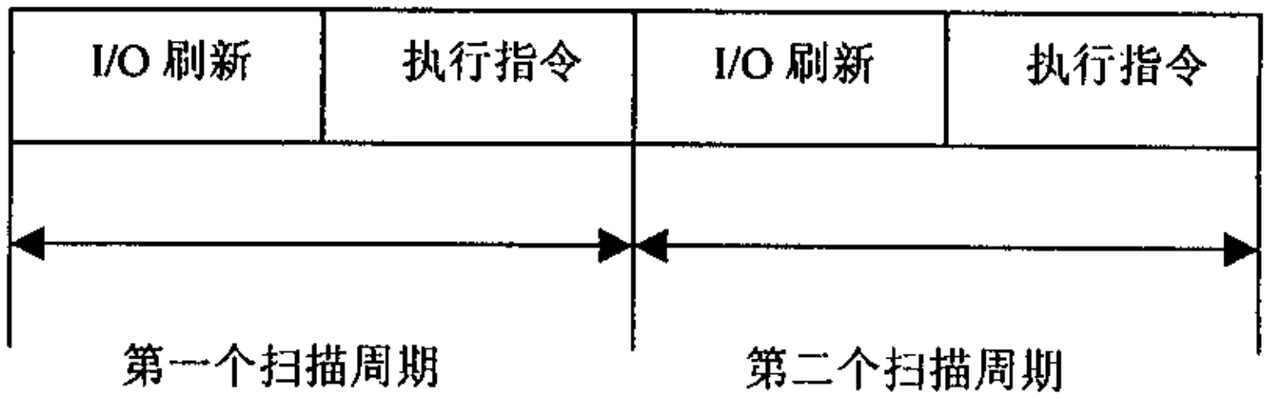


图 2.1.1.1　可编程控制器工作方式示意图

所谓 I/O 刷新即对输入进行一次读取，将输入端各变量的状态重新读入可编程控制器中存入内部寄存器，同时将新的运算结果送到输出端。这实际是将存放输入、输出状态的寄存器内容进行了一次更新，故称为“I/O 刷新”。

由此可见，若输入变量在 I/O 刷新期间状态发生变化，则本次扫描期间输出端也会相应地发生变化，或者说输出对输入产生了响应。反之，若在本次 I/O 刷新之后，输入变量才发生变化，则本次扫描输出不变，即不响应，而要到下一次扫描期间输出才会产生响应。由于可编程控制器采用循环扫描的工作方式，所以它的输出对输入的响应速度要受扫描周期的影响。

总之，采用循环扫描的工作方式，是可编程控制器区别于微机和其他控制设备的最大特点。

2.1.2　S5-135U 的硬件结构

可编程控制器的基本系统

可编程控制器的基本系统方框图如图 2.1.2.1 所示。这个基本系统有中央处理器组件、存储器组件、数字量和模拟量输入组件、数字量和模拟量输出组件、外围设备接口和编程器接口组成，并由总线连接起来。

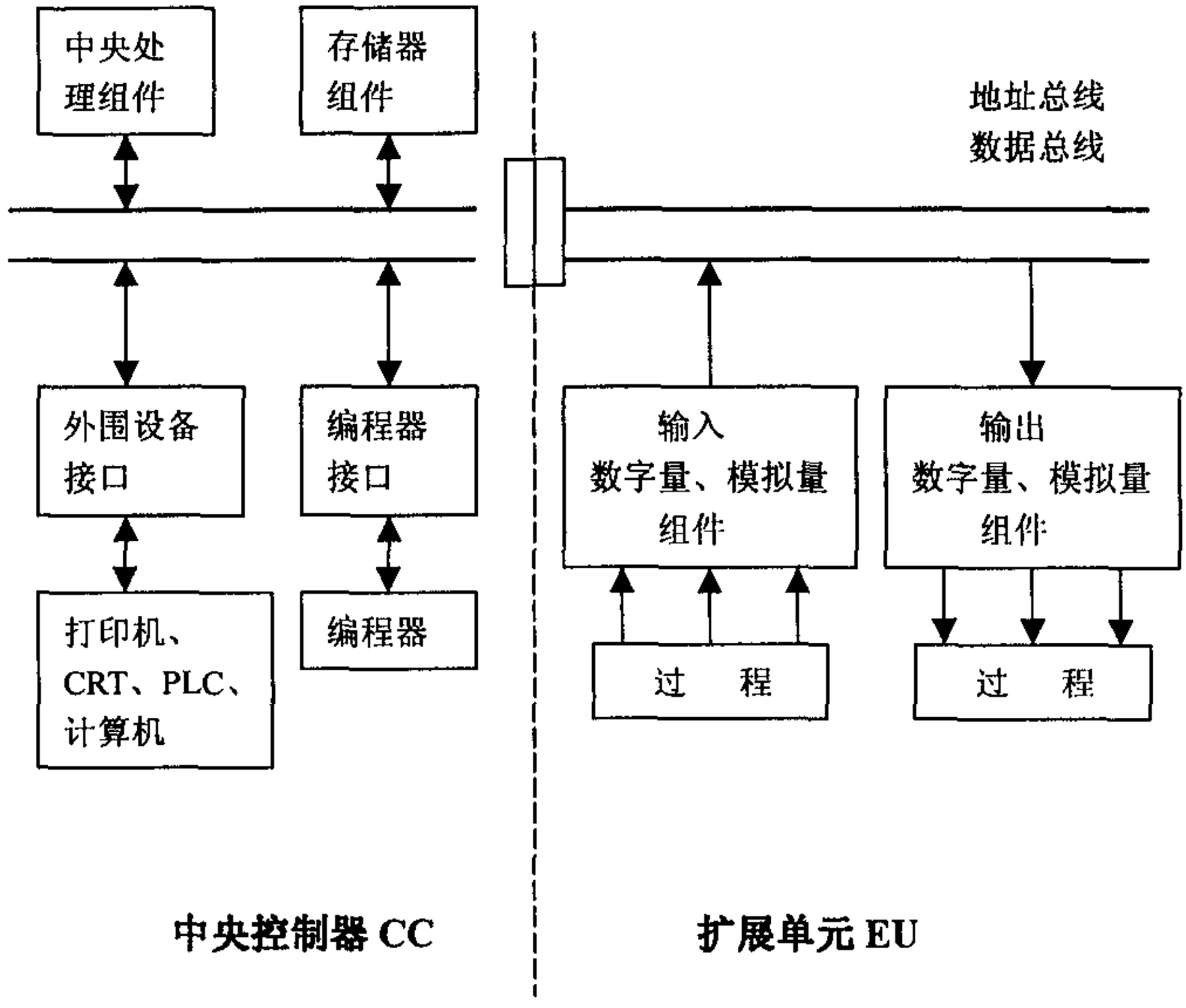


图 2.1.2.1 可编程控制器系统框图

S5-135U 的硬件结构

S5-135U 由中央控制器和扩展单元组成。中央控制器由中央组件、电源、数字量输入输出组件、模拟量输入输出组件、接口组件通信组件和智能组件等构成。在中央控制器的输入输出点不够时，可通过扩展单元实行扩展。S5-135U 硬件结构框图如图 2.1.2.2 所示。

通过通信模板 CP525 可与打印机、键盘、CRT、计算机和其它可编程控制

器连接；通过 CP143TF 可与 SINEC-H1 连网。

要实现可编程控制器的通信及各种控制功能，还必须由用户按照规定的语言和程序结构编制用户程序，并把它输入控制器。为此，可编程控制器的制造厂商开发了专用的语言。该语言既适用于逻辑、计时、计数、比较等控制，又以它特有的为各类人员所熟悉的表达方式使得编程简单、使用方便。

SIEMENS 公司为 S5 系列开发了 STEP 5 语言，它们具有共同的特点：

- 有语句表（A）、梯形图（K）和功能图（F）三种语言表达形式，较高级的编程方式还有图形编程（GRAPHIC），需要相应的配套软件；
- 有相似的参数表示形式；

S5-135U 的程序都可采用单元的程序结构进行编程。下面具体阐述 S5-135U 程序编制。

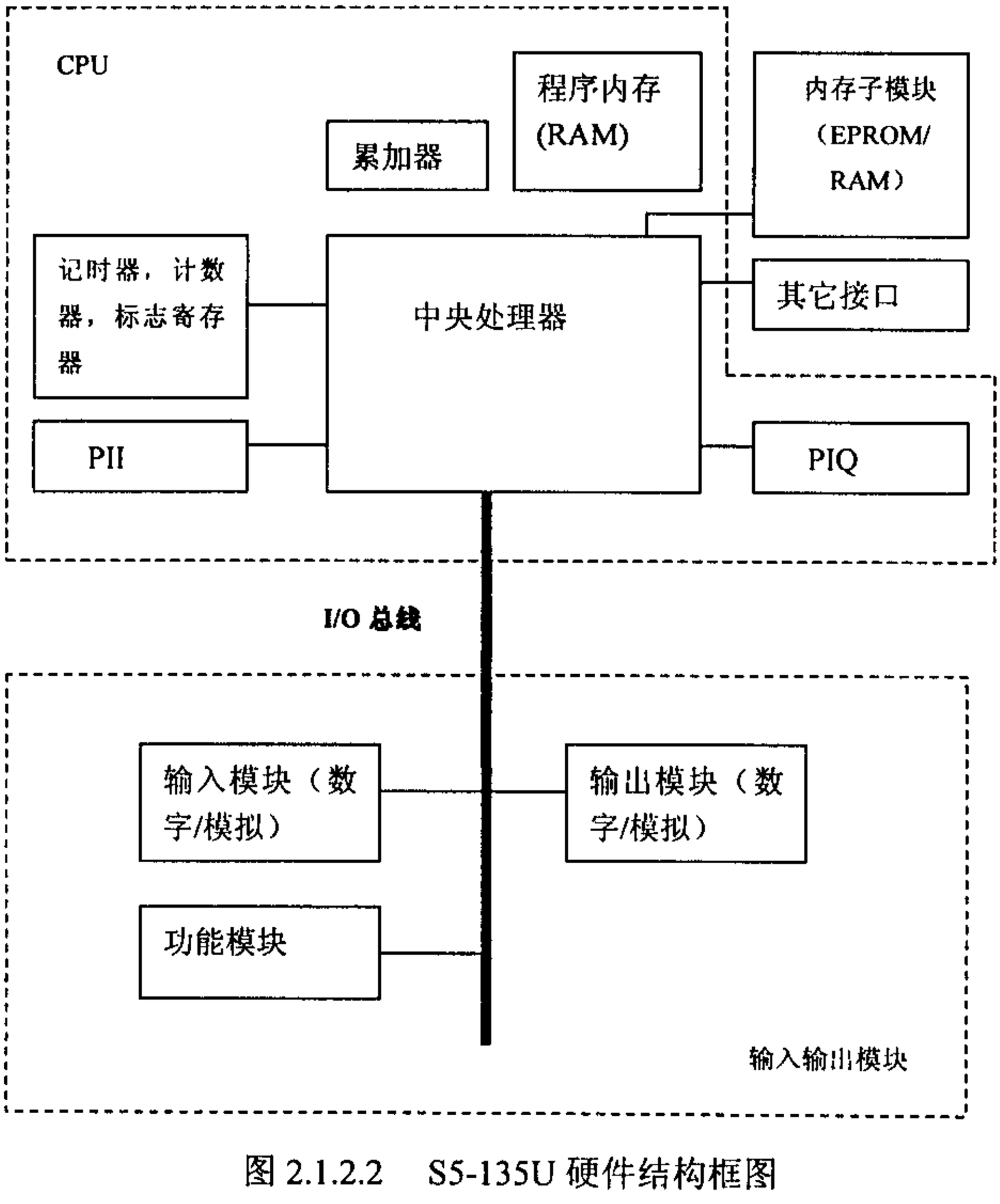


图 2.1.2.2　S5-135U 硬件结构框图

2.1.3 S5-135U 程序的编制

S5-135U 可编程控制器要求用户采用结构化编程技术，也就是把程序分成若干自成一体的程序段(称为单元)。这种方法有下列优点：编程简单和清晰，尤其适用于较大的程序；使程序单元标准化；简化程序管理；易于修改；程序测试方便；容易投入。

用户程序的构成包括用于不同任务的各种单元：

管理单元（OB），用于用户程序的管理。

程序单元（PB），用于把用户程序按工艺分类。

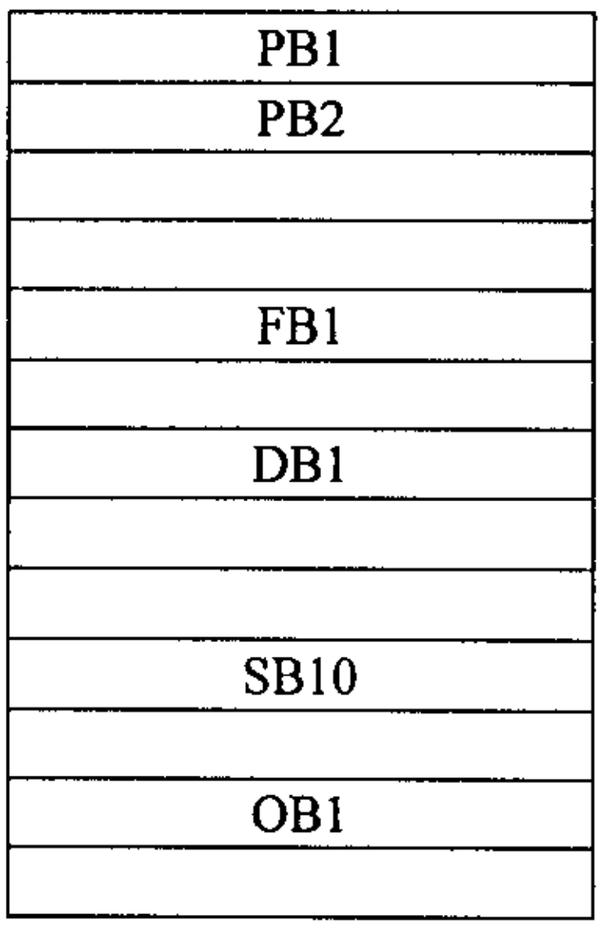
功能单元（FB），用于重复使用的、复杂的功能编程（例如开环控制、闭环控制、报警和计算功能）。

顺序单元（SB），用来完成顺序链的专门形式的程序单元。

数据单元（DB），用于数据和文本的存贮。

每种单元最多可用到 255 个，而每个单元不超过 256 条语句。由编程器把全部单元以任意次序寄存在程序存储器中，见下图。

用户只需对管理单元编程，那么，管理单元就确定个单元应当执行的次序。



程序单元和功能单元的执行次序由管理单元确定，为此在管理单元中编制相应的单元调试(有条件或无条件)。管理单元也如其他单元一样存储在存储器中，各种不同的管理单元用于各种不同的程序处理。

程序单元、功能单元和顺序单元能以任意组合进一步调用程序单元、功能单元和顺序单元。最多允许的单元嵌套数包括管理单元在内为 8 级，但不包括被调用的数据单元。

图 2.1.3.1 所示为最多嵌套的程序结构的例子：

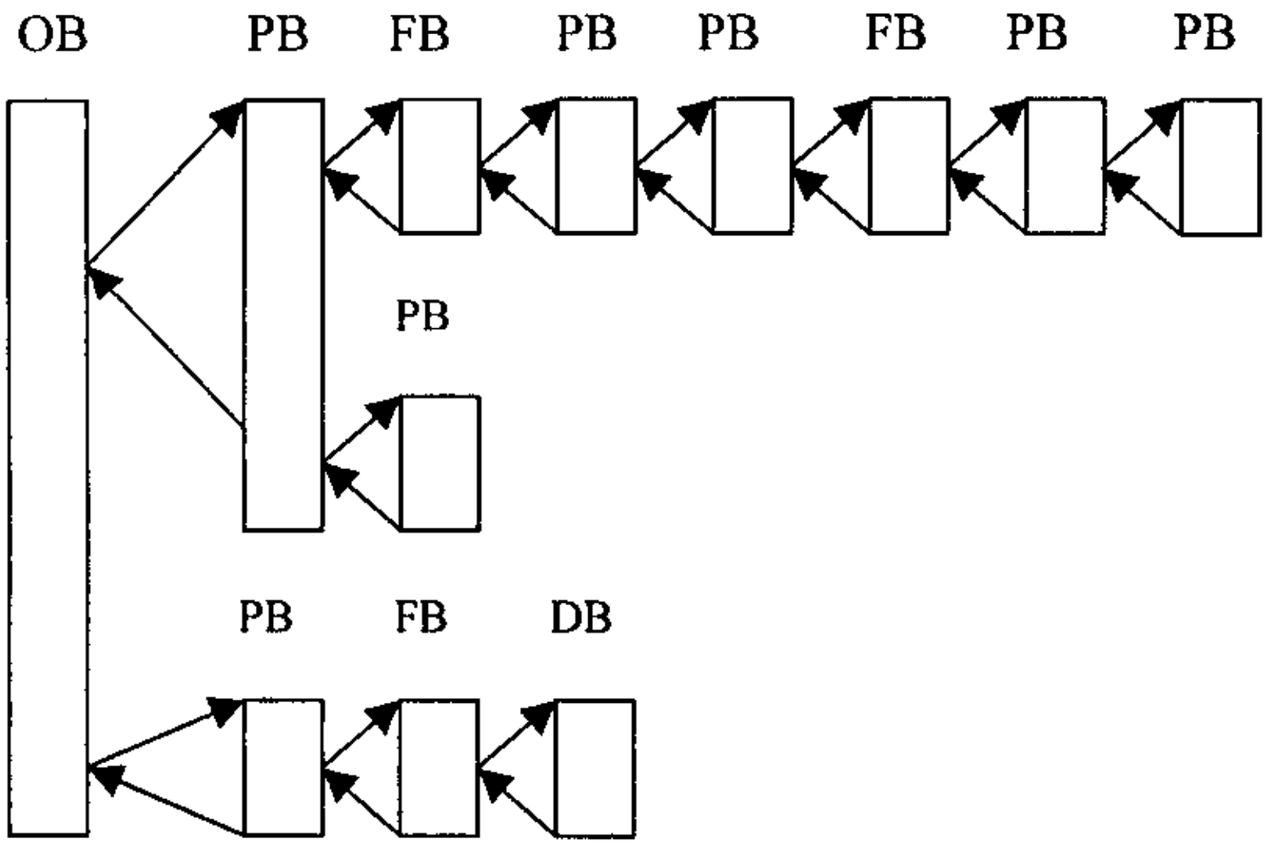


图 2.1.3.1　最多嵌套的程序结构的例子

● 程序单元

程序单元能用基本指令编程，它能用 STEP 5 语言的三种表达方式（STL，CSF，LAD）写入或读出。程序单元编程是以指定程序单元号（1~255）开始的，最后以语句 BE 结束。程序单元最多为 256 条语句，超过极限的语句是无效的。

程序单元的处理是通过单元调用来达到的。这种调用能编在管理程序或功能单元中，与转移子程序相似。它既能实现无条件转移，又能有条件转移。在语句 BE 之后，程序转回到原来调用的程序，调用后或在 BE 之后，逻辑结果不再进行处理，而是带到新单元并计值。

● 数据单元

数据单元 DB 用于存放用户程序所需要的数据。数据可以是下列的类型：任何的位模（如作为设备状态表示）；数值（十六进制、二进制、十进制）；数字文字符号（如作为信息文本）。

在数据单元编程的开始，用 1~255 来定数据单元号（如 DB25）。每个数据单元最多可由 256 个数据字（16）位构成，见图 2.1.3.2：

数据单元（DB）只能无条件调用，在新的单元调用之前，老的单元调用一直保持有效。

数据单元的调用可以在程序单元、功能单元或顺序单元中编程。

● 功能单元

功能单元和程序单元一样是用户程序的一部分。然而与程序单元相比有 4 个主要差别：

1.功能单元可指定参数，也就是能预先给出实际操作数，并使用这些操作

数进行处理。

2.功能单元能用补充指令库进行编程

3.功能单元的程序只能用语句表来编程。

4.功能单元在用户程序中表达复杂的、封闭的功能。

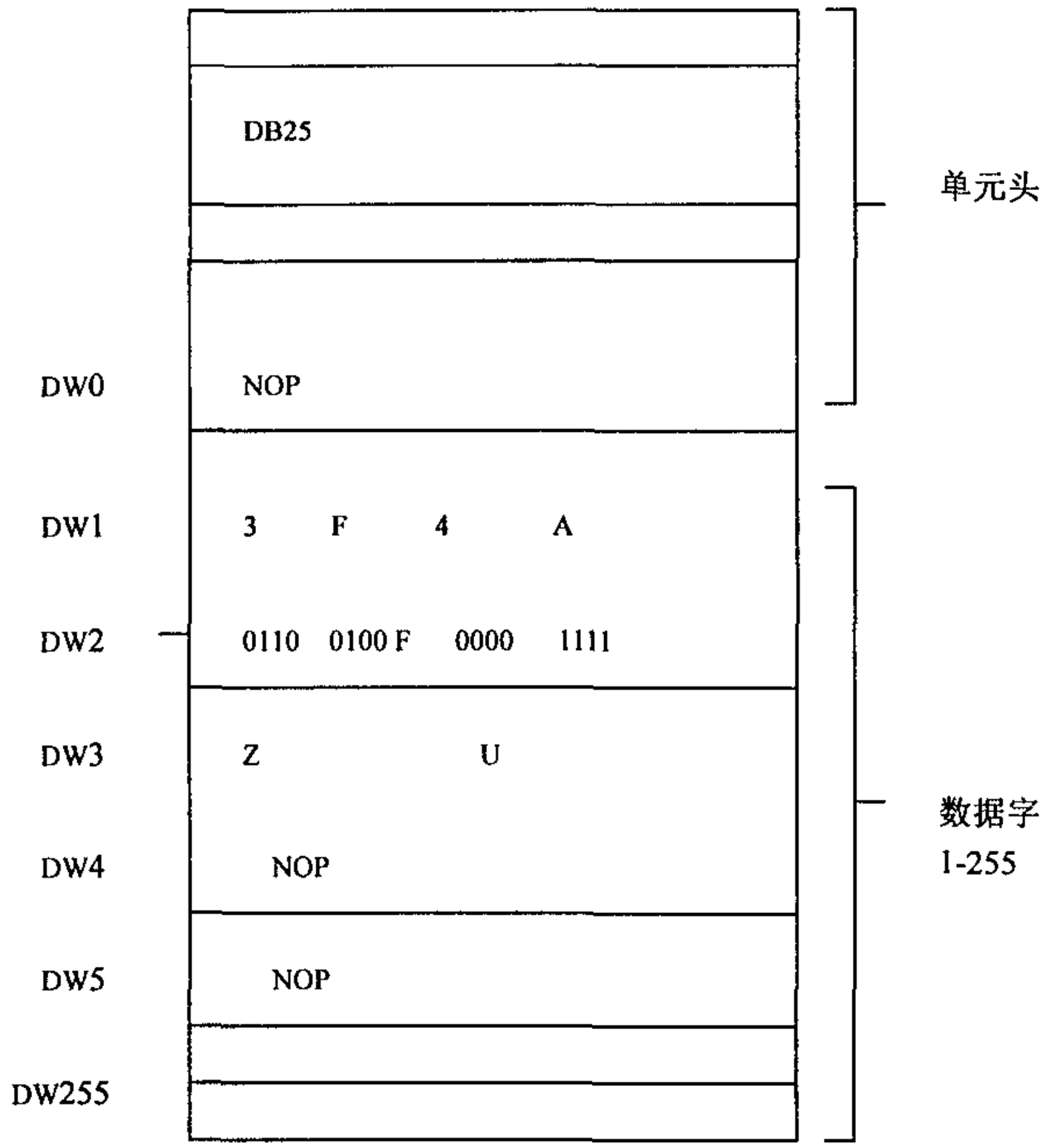


图 2.1.3.2　数据单元的结构

● 管理单元

可编程控制器的全部程序由系统程序和用户程序所组成。系统程序是有关内部操作功能的全部语句和说明，它是控制器的一个固体组件（EPROM），不允许用户变更。系统程序和用户程序之间的接口是管理单元。管理单元虽然也是用户程序的一部分，但它只能由系统程序来调用，用户不能调用管理单元，然而用户能够通过编程来间接影响系统程序。管理单元也如程序单元那样编程。

2.1.4 CPU928 内存的组织与分配

CPU928 的内存主要分为以下几个区：

- 用户存储区：用来存放用户程序，即 OB、FB、PB、SB 等块的存储区，16 位宽，存储区大小为 32×2^{10} 字。分配地址为 0000~7FFF。
- DB-RAM 区：用来存放数据块 DB（DB0 除外）的存储区，16 位宽，大小为 23×2^{10} 字。分配地址为 8000~DD7F。
- DB0 区：DB0 专用存储区，16 位宽，分配地址为 DD80~E3FF。DB0 中存储了所有程序块的首地址。
- S 标志区：8 位宽，大小为 1024 字节。分配地址为 E400~E7FF。
- 系统区：16 位宽，用来存放系统传输数据（RI/RJ 区，各为 256 字）、系统数据（RS/RT 区，各为 256 字）、计数器（256 字）及计时器（256 字）。分配地址为 E800~EDFF。
- F 标志区：8 位宽，大小为 256 字节。分配地址为 EE00~EEFF。
- PII 及 PIQ 区：用来存储过程输入输出映像。8 位宽，各占 128 字节。分配地址为 EF00~EFFF。
- 外围设备 I/O 区：8 位宽，大小为 4×2^{10} 字节。分配地址为 F000~FFFF。

2.2 系统结构分析与设计

在组建现场总线控制系统（FCS）时，我们应充分考虑系统的稳定性、可扩展性以及性价比等因素。要实现高性能的通信网络，现场总线技术必不可少。目前现场总线标准众多，它们各具特色，适用于不同的领域。因此在短期内不可能形成统一的标准的局势下，选用何种网络产品，就需要根据应用的具体要求而定。

本项目中采用 SIEMENS 公司的 SIMATIC SINEC 系列可编程控制器网络构成整个系统，它提供四种常用的独立网络：远程 I/O 系统，SINEC-L1，SINEC-L2 及 SINEC-H1。其中 H1 网为高速工业局域网，采用工业以太网协议，其传输速度高达 10Mbps。L2 网以 PROFIBUS 协议为基础，实现与现场设备的实时通信任务。PROFIBUS 是一种国际性的开放性现场总线标准，是由以西门子为主的十几家德国公司共同推出的，并在欧洲得到广泛的应用。有关 PROFIBUS 的具体内容请参见第 3 章。

在早几年的 S5 网络中，常由 SINEC-H1，SINEC-L1 及远程 I/O 系统三级子网构成复合结构，实现西门子的四层金字塔。SINEC-L1 是一种价格比较便宜的现场网络，采用主从方式管理通信。它适用于对时间没有苛刻要求的控制过程，可实现集中监控。笔者从系统的冗余度及可升级角度考虑，采用实时性更佳的 SINEC-L2 网取代 L1 网，从而组建了由 SINEC-H1，SINEC-L2 及远程 I/O 系统三级子网构成的复合结构。如图 2.2.1 所示。

根据系统的复杂程度，西门子的 S5-135U 可编程控制器是比较适宜的，它采用模块式结构，便于今后的维修及升级。由于任务的多样化及处理的实时要求，采用了两块 CPU 分别作为通用控制处理器和级联控制器，两者通过一个协

处理器通信。另外由于控制点数较多，采用了大量的现场级 I/O 模板 ET200 及接口模板 IM308B 构成远程 I/O 系统。系统的硬件结构如图 2.2.2 所示。

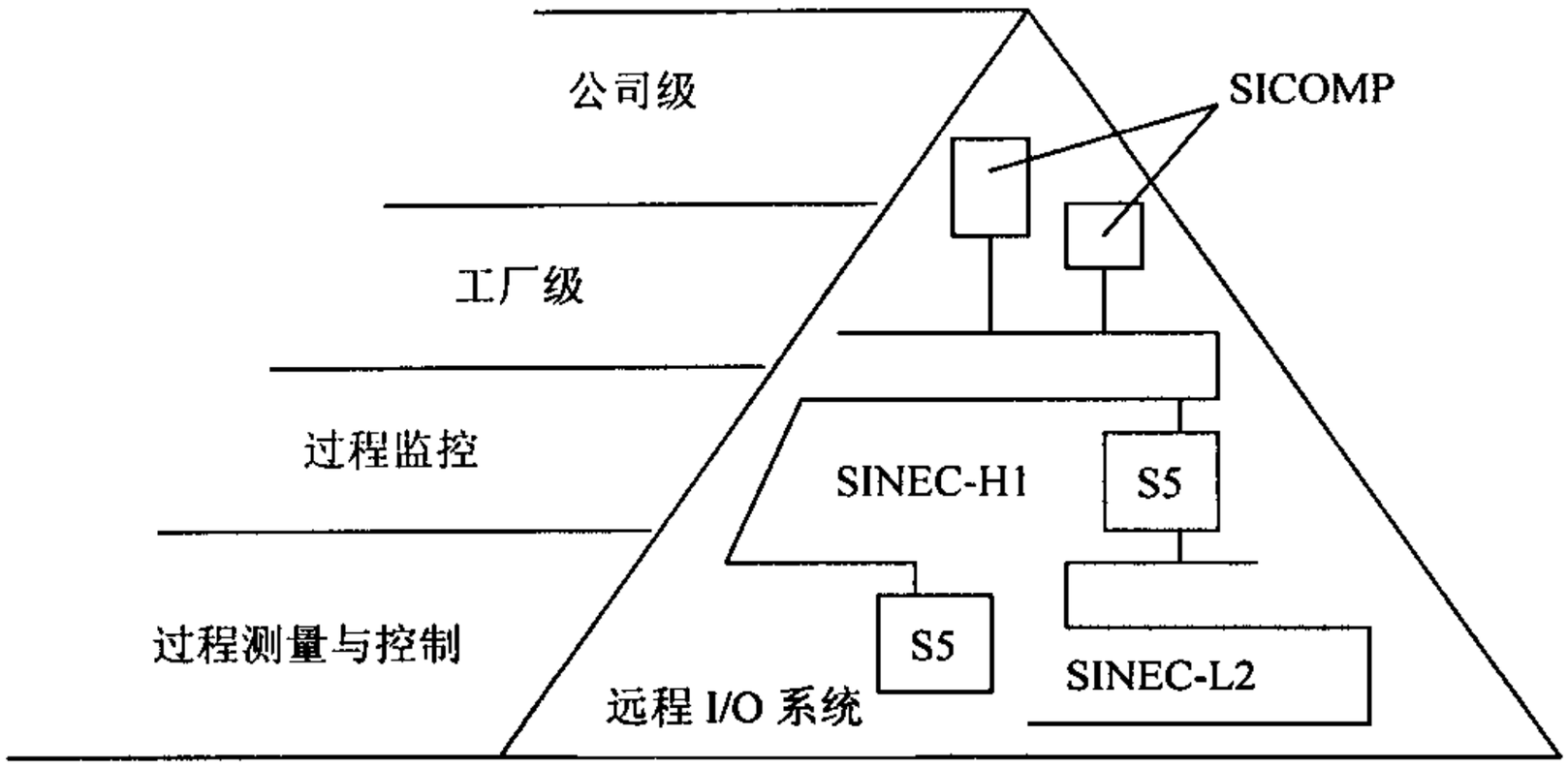


图 2.2.1 西门子 S5 四层金字塔网络结构

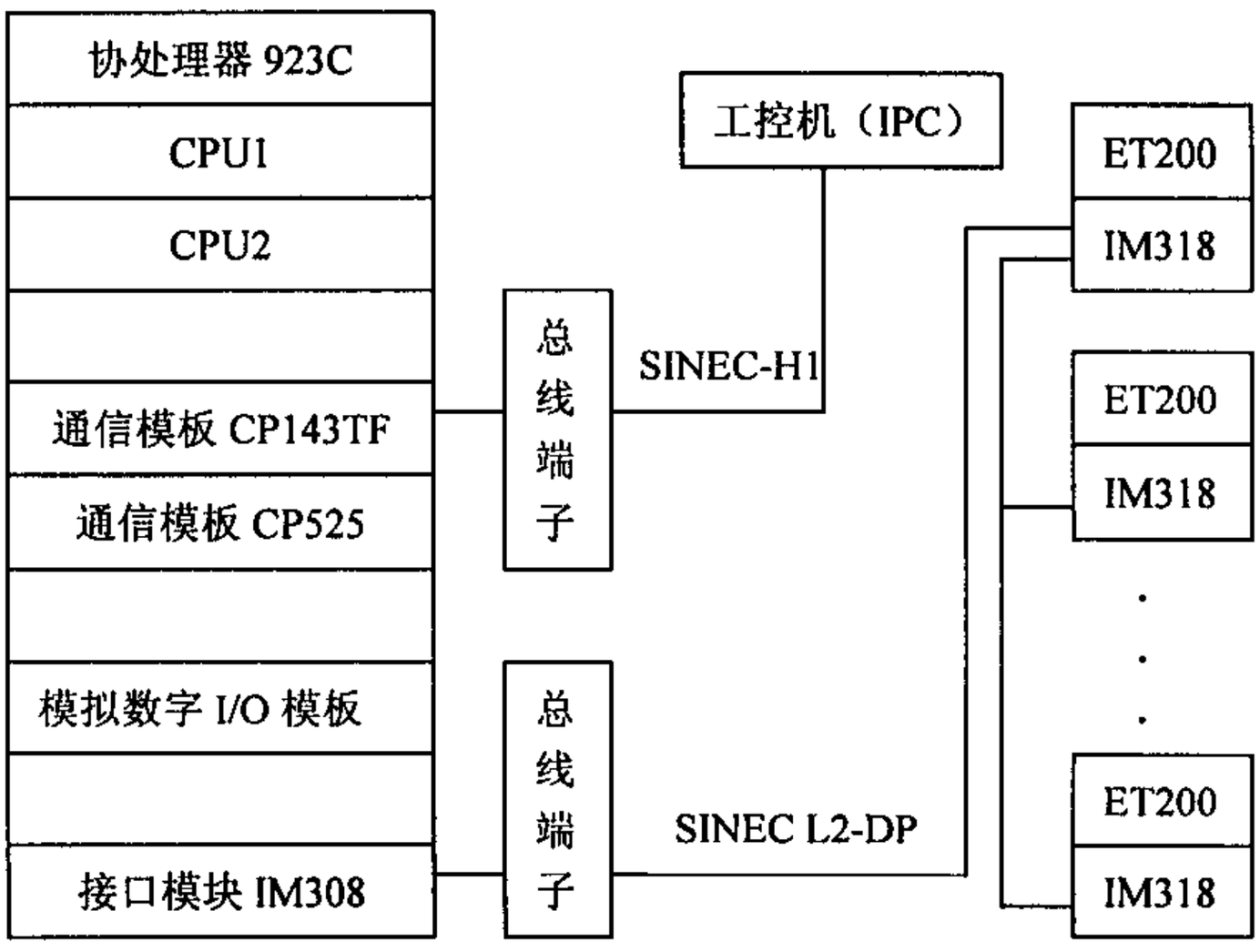


图 2.2.2 系统硬件结构

现对图 2.2.2 中相关模板简要说明如下。

S5-135U：大型 PLC，模块式结构，是过渡型产品。采用多处理器运行，

本系统中配置了两块 CPU928 处理器及一个协处理器 923C。

ET200：现场级的 I/O 模块，有数字和模拟之分。它们挂在 SINEC-L2 总线上，通过总线与 CPU 中的 PII 区（Process Image of Input，过程映像输入）和 PIQ 区（Process Image of Output，过程映像输出）交换数据。

CP143TF：用于 SINEC-H1 网的专用通信模板。驻留了 OSI 模型的全部 1~7 层协议，并提供两种接口，其中 1~4 层支持传输接口，而 1~7 层支持 TF 接口。有关内容请参见第 4 章。

CP525：通信处理器模板，提供两个 V.24（RS232C）接口/20mA 电流环（TTY）接口，必须在 S5-DOS 下用 COM525 编程后方能使用。

IM308—IM318：接口模板对，用于范围 3000 米之内，串联式远程 I/O 系统。IM308 上有两个接口，每个接口最多可连接 32 个扩展机架或 ET200。有关远程 I/O 系统请参见本章后面的内容。

SINEC-H1：相当于 S7 中的工业以太网，兼有工业控制局域网与办公自动化网的特点。有关 SINEC-H1 的详细内容请参见第 4 章。

SINEC-L2：采用 PROFIBUS 协议（详细内容参见第 3 章），与 S7 系列的 PROFIBUS 现场总线相兼容。它与 SINEC-H1 的组合成为近年来西门子 S5 系列互联通信的最主要的网络。有关 SINEC-L2 的详细内容请参见第 5 章。

2.3 数据管理功能块（DHB）

西门子 S5 系列工业局域网的通信是通过两级数据交换实现的，一级是发生在同一台可编程控制器之内的 CPU 模板与 CP 通信模板之间的数据交换，另外一级是指在 PLC 网络上，不同的 PLC 的 CP 通信模板之间，经由网络实现的数据交换。前者是通过调用 DHB（data handling block），经由一个双口存储器作桥梁（共享区）实现的数据交换，这是一种并行通信。利用 DHB 不仅可以实现 CPU 与 CP 之间的数据交换，而且还可以实现 CPU 与各种智能模板之间的数据交换。从这个意义上讲，DHB 的使用具有通用性，因此单独加以介绍。

西门子 S5 系列可编程控制器共有 6 个 DHB，这些功能块必须相互配合才能实现通信功能。为了保证其模板通用性，DHB 采用形式参数编程，在调用时必须对形式参数赋值，变为实际参数。这类似于 C 语言中的函数。

完成一个通信过程，常常需要按一定的顺序及呼应关系调用几种 DHB。对于不同类型的可编程控制器，功能块的编号有所不同。

在 S5-135U（CPU928）中：

FB120：SEND 块，用来启动向 CP 模板发送数据的作业；

FB121：RECEIVE 块，用来启动对传送来的数据进行接收的作业；

FB122：FETCH 块，用来启动一个作业，从网络上的目的站读取数据，再经网络取回自身的 CPU 模板，这时 CPU 应当用 RECEIVE-ALL 接收取回的数据；

FB123：CONTROL 块，用来更新特定作业的作业状态字或者给出正在执行的作业的作业号；

FB124：RESET 块，用来对指定接口正在执行的作业或者全部作业复位；

FB125：SYNCHRON 块，在启动 PLC 时，用它使 CP 或智能模板与 CPU 模板同步，并对 CP 与智能模板的接口进行初始化，以保证 DHB 正常运行。

下面将进一步说明 DHB 的使用。

2.3.1 DHB 的参数描述

每种 DHB 都要用到一些形式参数，归纳结果如表 2.3.1.1 所示。其中 I=输入参数，Q：输出参数，D：数据，BY：字节地址，W：字地址，KY：两个绝对数，KS：两个字符，KF：定点数。

表 2.3.1.1　DHB 形式参数汇总表

参数名称	参数类型	数据类型	说明
SSNR	D	KY	接口号（页面号）
A-NR	D	KY	作业号
ANZW	I	W	作业状态字（双字）
QTYP/ZTYP	D	KS	数据源/数据宿的类型
DBNR	D	KY	数据块的编号
QANF/ZANF	D	KF	数据源/数据宿的开始地址
QLAE/ZLAE	D	KF	数据源/数据宿的长度
PAFE	Q	BY	参数赋值出错的错误标志
BLGR	D	KY	数据帧的最大规模

SSNR：接口号。CPU 模板与通信模板之间采用共享存储器通信法交换数据，共享区是通信模板中的双口 RAM。为了支持可编程控制器的多处理机运行有些通信模板把双口 RAM 共享区划分为多个页面，每个页面作为一个接口，供其中一个处理机与此通信模板交换数据用。接口号的范围是 0~255，一经设定，DHB 在调用时必须按设定值调用。接口号本质上是个地址。

A-NR：作业号。用来定义通信模板上的一个独立作业，它不表示地址，而表示选择要执行什么作业。

ANZW：作业状态字。用来确定目前作业进行的状态。

QTYP/ZTYP：数据源/数据宿的类型。要求用两个字母字符赋值，有直接和间接赋值两种赋值形式。

DBNR：数据块的编号。当 QTYP/ZTYP 为间接赋值时，用 DBNR 指定所涉及的数据块的编号。若 QTYP/ZTYP 为直接赋值，DBNR 无意义。

PAFE：错误标志。参数赋值的各种错误都记录在 PAFE 中。

BLGR：数据帧的大小。仅仅用在同步块，规定了通过 DHB 一次能交换的数据帧的最大字节数。

2.3.2　DHB 的调用及其配合关系

在利用 DHB 编制用户通信程序时，必须恰当地进行几种 DHB 的配合调用，才能顺利完成通信任务。例如，在 OB20，OB21，OB22 中必须调用 SYNCHRON 功能块进行 CP 与 CPU 同步并且进行通信模板接口初始化，只有在执行了同步块之后，DHB 调用才能正常执行。

图 2.3.2.1 表示了要通过 DHB 功能块的调用，实现从 CPU1 经网络向 CPU2 传送数据的过程。在 CPU1 中要完成发送任务，则应以 SEND 块为核心，再配合调用 SYNCHRON 块，CONTROL 块及 RESET 块。而在 CPU2 中要完成接收任务，则应以 RECEIVE 块为核心，再配合调用 SYNCHRON 块及 CONTROL 块。

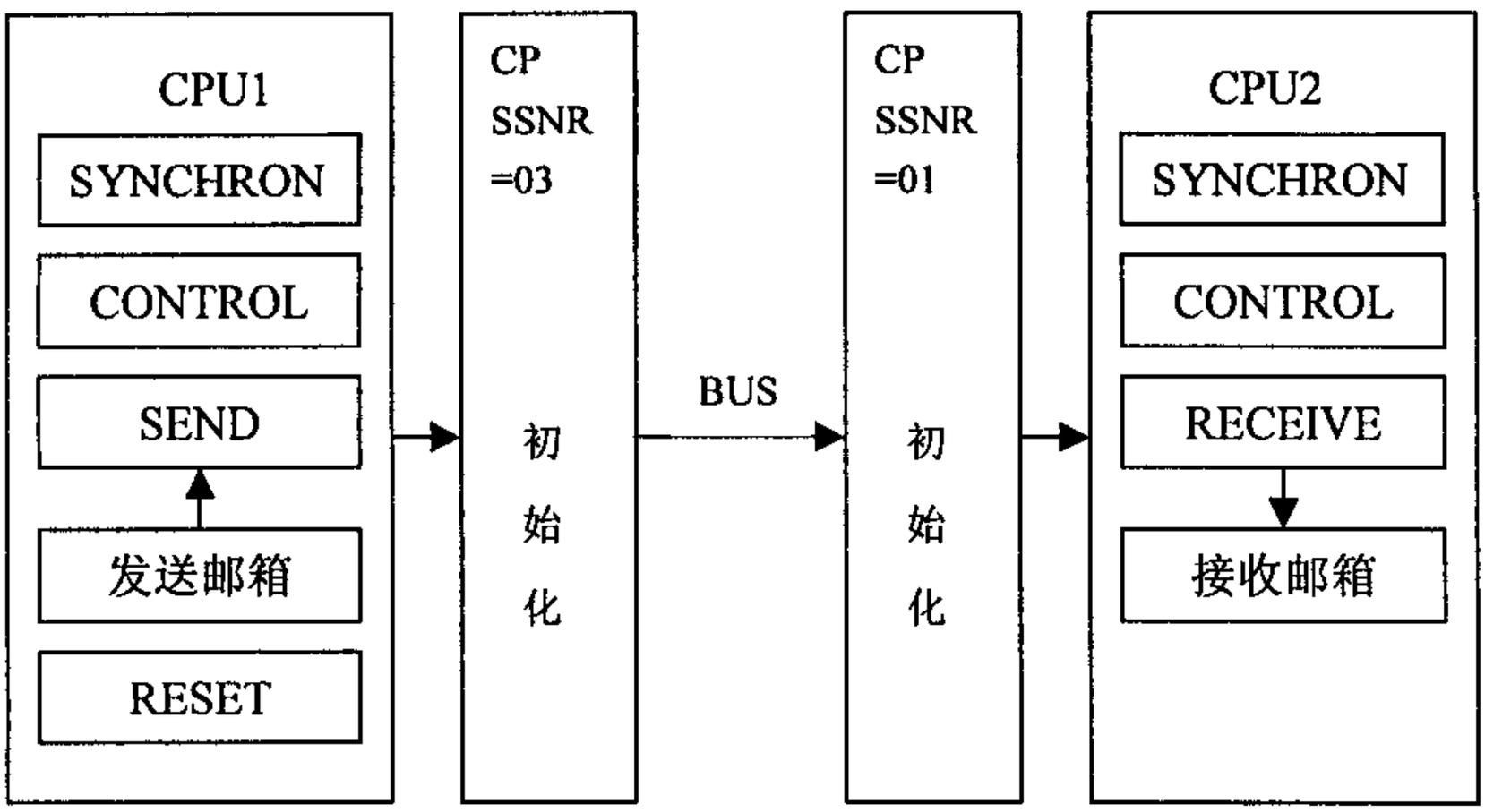


图 2.3.2.1　DHB 调用配合关系示例

2.4 S5-135U的远程I/O系统

由单台可编程控制器构成的控制网络，根据现场I/O点的分散程度及控制器与现场I/O点的距离远近，可以采用集中式结构或者分散式结构。

本系统中由于中央控制器与扩展单元相距较远，且中央控制器与ET200站分别安装在不同机箱内，所以选用了分散式结构。这种结构的特点是中央控制器与扩展单元之间采用串行通信，分散式结构构成的系统又称为远程I/O系统。

2.4.1　通信原理及特点

在S5系列的可编程控制器远程I/O系统中，插在中央机架上与插在扩展机架上的远程接口模板之间通过电缆或光缆连接成主从式总线系统。中央机架上的

远程接口模板为主机，各扩展机架上的远程I/O模板为从机。在主机中建立远程I/O缓冲区，由主机采用周期轮询方式与各从机交换数据，对远程I/O缓冲区进行更新。而中央机架上的中央处理器只需访问设在本地的远程接口模板内的远程I/O缓冲区就实现了与远程I/O单元的通信。这种通信方式又称为“周期I/O方式”。

与美国及日本相比较，西门子S5系列的远程I/O系统是严格符合定义的，其从站只能是远程I/O单元。而且其构造也是最为复杂的，这表现在它的机架类型最多，接口模板更多，并且还要进行开关设置及跨接线连接。远程I/O系统作为远程I/O点信号的采集系统，一般通信距离不会很远，然而西门子公司为其S5系列的远程I/O系统设计了各种规格，其通信距离有200m，600m，1000m，3000m几种。通信介质有电缆与光缆，从这个意义上讲西门子的远程I/O系统是规格最全的。在使用上，这些I/O系统是极其相似的，只要对远程I/O进行正确的地址分配，那么主站使用读写指令对这些地址进行直接操作就实现了远程通信。

2.4.2　远程I/O系统结构分析

S5-135U的I/O系统从结构上来看分为集中型与分散型两种。集中型结构的通信距离比较短，一般限定在0.5~2.0m之内。而分散型结构通信距离较长，根据选取的接口模块的不同，通信距离可达200m，600m，1000m，3000m甚至更长（选用光缆连接，IM307——IM317接口模块对），是构成远程I/O系统的理想结构，使得I/O模块深入到现场的每一个角落。

鉴于此，并考虑到应留有一定的冗余度，以方便今后的扩展和升级，我们采用了通信距离可达3000m的串联分散型结构，接口模块选用了IM308—IM318的搭配。具体连接参见图2.4.2.1。

在中央机架上安装了两块IM308接口模块，它们通过总线端子与SINEC-L2网相连。其中一块用于连接ET200站，另外一块通过X105接口与机械设备的控制变频器相连，以实时采集现场数据。每块模板上有两个接口，每个接口最多可接32个扩展机架或ET200。

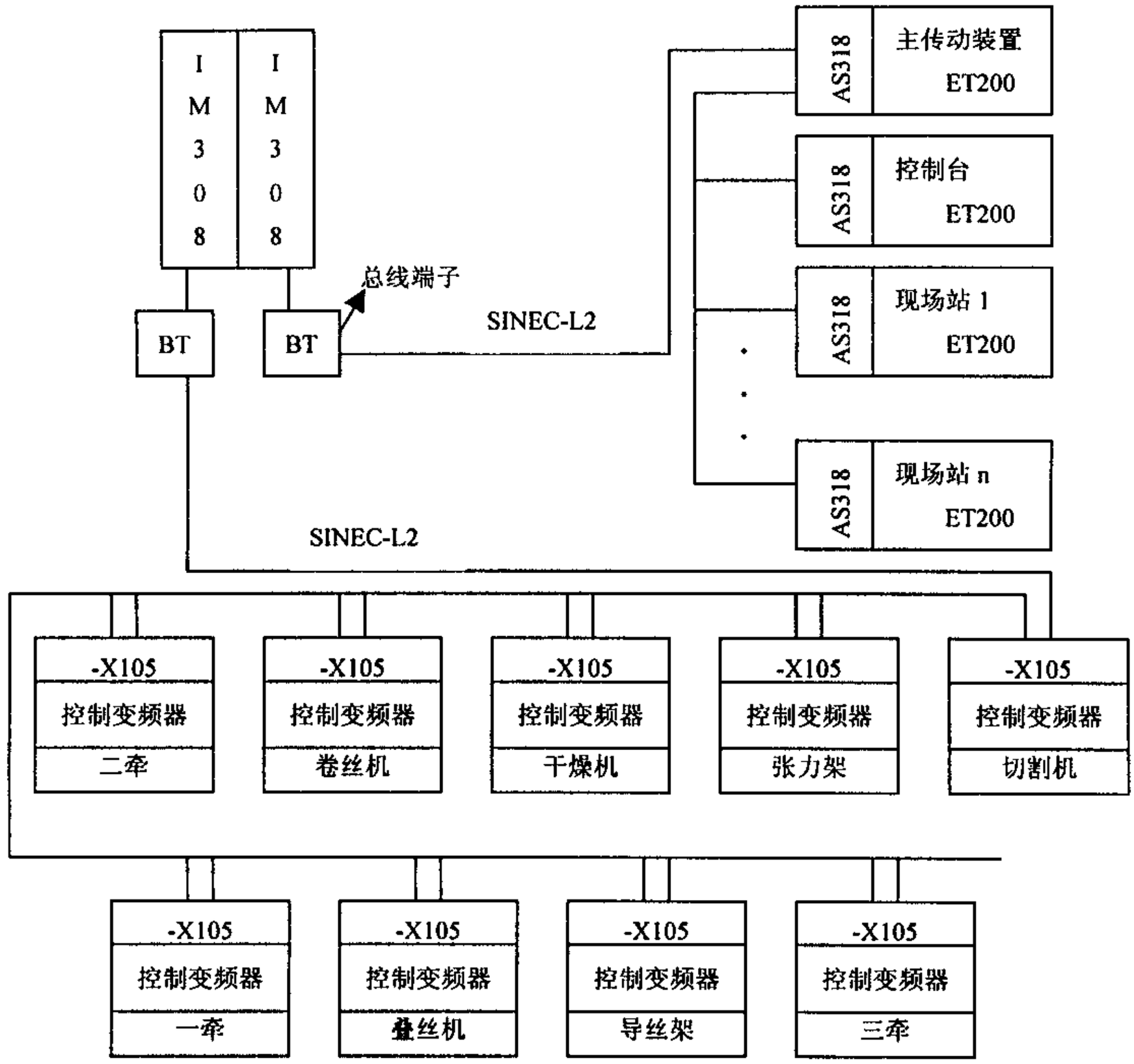


图 2.4.2.1　远程 I/O 系统结构

3　现场总线技术及 PROFIBUS

3.1 现场总线技术概述

随着计算机、通信、网络等技术的发展，引发了自动化系统结构的变革，逐步形成以网络集成自动化系统为基础的企业信息系统。现场总线（Fieldbus）就是顺应这一形势发展起来的新技术。

3.1.1　总线技术应用概述

总线（Bus）的本来含义是二进制单元信息系统。可以将它理解为以信息传输软硬件为基础，以信息传输规范为核心的信息传输体系。它对于电子计算机的诞生和发展起了重要作用。一台计算机系统中含有许多总线。从系统的不同层次上看，有芯片级总线、板级总线、系统级总线等。从信息传输形式上看，有并行总线和串行总线之分。总线技术与通信技术有密不可分的关系。并行通信强调高速性，较多地依赖于硬件实现。计算机中最早应用的总线是并行总线。芯片内和芯片间的并行总线一般地按功能分为分数据总线、地址总线和控制总线，这些总线结构由芯片生产厂家自行设计，没有国际标准。为便于用户开发应用，系统级总线一般由计算机生产厂家独立或联合提出，然后形成国际标准，以对进一步的开发应用进行规范。这种总线由于传输距离短，通常称为局部总线（Local Bus）。

20 世纪 60 年代后串行通信技术得到发展，不久国际上推出了第一个串行通信标准，即 RS232 标准，出现了至今仍广泛应用的 RS232 串行总线。按 RS232 的最简单应用模式（即远距离通信模式），用三根导线可进行全双工串行通信，用两根导线可进行半双工串行通信。全双工即信息的接收和发送可以同时进行，半双工则指的是既可接收，也可发送，但二者不能同时进行。完整的 RS232 应用模式要用到一系列的握手信号线及电源线。与并行通信相比，串行通信需要对信号进行一系列的规定，称为串行通信协议，这比并行通信只需对引线端加以简单的定义和说明要复杂得多。串行通信除了信号通道少外，还要对需传输的数据进行规范化分解封装，加上发送者信息、接收者信息、数据块大小类型和序号、校验信息等等附加数据，附加的数据量通常比原本要传输的数据量大许多，所以比并行通信要慢很多。但是，串行通信的巨大优势是：线缆用量显著减少。对于远距离应用而言，这不仅降低了线路费用，而且由线缆极其连接故障造成的系统故障（也是最常见的系统故障）大大减少，系统的易维护性显著提高，维护费用大大降低。因此，在远距离通信上，毫无疑问要采用串行通信而不采用并行通信。

事实上，RS232 的物理结构并不是理想的串行通信结构，它采用单端输入输出方式，抗干扰能力差、通信距离近是其固有的缺点。80 年代初推出的 RS422 和 RS485，采用差动输入输出方式，使通信距离和性能大大提高（19.2kbps 时可传输 1200 米）。RS422 适用于全双工异步通信，需两对（4 根）导线；RS485 则专用于半双工异步通信，只需一对导线。在短距离串行通信方面，广泛用于

计算机同串行外设连接的 USB 是取得巨大成功的一个例子，它用 4 根导线实现短距离高速串行数据传输。芯片级串行总线则广泛应用 I2C 总线协议和三线式串行通信协议。

串行通信技术是构成网络技术的基石。网络技术的发展也对串行通信提出了更高层次的要求。上面提到的 RS232、RS422、RS485 等只提供了串行通信的最低层协议，即物理层协议。仅靠物理层协议只能完成功能最简单的串行通信。由于网络通信需要面对复杂的网络拓卜结构和遥远的通信距离，需要解决线路共享、冲突仲裁、中继转发、分组发送、路径选择、流量控制、接收重组、差错处理等等一系列技术问题，对这些问题的研究导致开放式互连（OSI）基本参考模式于 70 年代应运而生，并于 1983 年成为正式国际标准 ISO7498。70 年代初，美国国防部投巨资研究 Internet，TCP/IP 协议和开放式互连（OSI）基本参考模式就是研究的重要成果。TCP/IP 协议是一种适于复杂的互联网应用的串行通信协议。TCP/IP 协议与以太网的结合成为最成功的网络总线模式。但是由于互联网结构固有的复杂性，按 TCP/IP 协议传输数据需附加的数据量很大，传输大数据块时才有较高的效率，而对于传输通常较简短的控制信息、网上对话信息等，则传输过程的绝大部分时间用在附加数据上，技术上称为协议效率（Protocol Efficiency）低。好在网络具有良好的共享性和传输的高速性，对于普通应用来说时间上的开销一般并不构成经济上的负担和不可接受的时间延迟。这正是它得到广泛应用的根本原因。

将计算机应用于控制从一开始就是计算机研究的主要目的之一。最早时由于计算机非常昂贵，计算机控制系统采用集中式控制的系统结构。运算是这种系统的瓶颈，电缆线路繁杂是这种系统的外在特点。单个节点的故障常会导致整个系统瘫痪、故障不易检测和诊断、系统不易维护是这种系统结构的先天缺陷。同期并行发展、价位较低因而更为流行的，是由数字电路模块构成的直接数字控制（DDC）系统。当时计算机昂贵是采用集中结构的唯一理由。

进入 80 年代后，计算机技术飞速发展，价位迅猛下降，使计算机在控制系统中的应用迅速普及。发展至今，单片机技术的推广使设备上电子测控系统的设计几乎成为嵌入式微机测控系统的一统天下。控制系统的结构向着理想的全分布式系统迅速靠近。1983 年美国的 Honeywell 公司推出了在标准模拟 4—20mA 变送器上附加数字信号传输的变送器，引发了智能变送器研究的热潮和相关技术的迅速发展。这件事情更大的意义在于：它将工控技术领域的关注点引向了串行通信。业内技术界似乎突然发现，工控技术竟然与串行通信技术有着如此密切的关系—全分布测控系统的实现要依赖于发挥串行通信的潜力。人们领悟到，过去一直采用的一对导线传输一路信号的典型解决方案仅对较高频率的信号传输才恰如其分，而对于通常的低频工业信号的传输则是对线缆资源的巨大浪费。频率越低，浪费越严重。人们注意到，利用高质量的串行通信，实现便于故障诊断和维护、能大大降低运行维护成本的全分布式测控系统，是一种相当理想的方案。以德法为首的欧洲最先提出了现场总线（Field Bus）的概念并大力投入研究，美国随后也迅速参与竞争，形成了从 80 年代持续至今的

现场总线技术群雄割剧的战国局面。

3.1.2 现场总线特点

现场总线是应用在生产现场、在微机化测量控制设备之间实现双向串行多节点数字通信系统，也被称为开放式、数字化、多点通信的底层控制网络。现场总线技术将专用微处理器置入传统的测量控制仪表，使它们各自都具有了数字计算和数字通信能力，采用可进行简单连接的双绞线等作为总线，把多个测量控制仪表连接成网络系统，并按公开、规范的通信协议，在位于现场的多个微机化测量控制设备之间以及现场仪表与远程监控计算机之间，实现数据传输与信息交换，形成各种适应实际需要的控制网络系统。现场总线使自控系统与设备具有了通信能力，把它们连接成网络系统，加入到信息网络的行列。

现场总线打破了传统控制系统的结构形式。传统模拟控制系统采用一对一的设备连线，按控制回路分别进行连接。而现场总线系统由于采用了智能现场设备，能够把原先 DCS 系统中处于控制室的控制模块、各输入输出模块置入现场设备，加上现场设备具有通信能力，现场的测量变送仪器可以与阀门等执行机构直接传送信号，因而控制系统功能能够不依赖控制室的计算机或控制仪表，直接在现场完成，实现了彻底的分散控制。由于采用数字信号代替模拟信号，所以可实现一对电线上传输多个信号，同时又为多个设备提供电源。

现场总线系统在技术上具有以下特点：系统的开放性、可互操作性与互用性、现场设备的智能化与功能自治性、系统结构的高度分散性以及对现场环境很强的适应性。

由于现场总线的以上特点，特别是系统结构的简化，使得这种技术具有诸多优越性。具体体现在：节省硬件数量与投资、节省安装费用、节省维护开销、用户具有高度的系统集成主动权以及系统的高准确性与可靠性。此外，由于它的设备标准化，功能模块化，因而还具有设计简单，易于重构等优点。

现场总线是当今自动化领域技术发展的热点之一，被誉为自动化领域的计算机局域网。它的出现，标志着工业技术领域又一个新时代的开始，必将对该领域的发展产生重要影响。

3.2 OSI 参考模型与现场总线通信模型

国际标准化组织 ISO 制定的 OSI 参考模型作为实现开放系统互连的分层模型，已为大家所熟知。其目的是为异种计算机互连提供一个共同的基础和标准框架，并为保持相关标准的一致性和兼容性提供共同的参考。具有七层结构的 OSI 参考模型可支持的通信功能是相当强大的。一个通用参考模型，需要解决各方面可能遇到的问题，因此应具备丰富的功能。作为工业控制现场底层网络的现场总线，要构成开放互连系统，应该如何选择通信模型？是否因需要实现 OSI 的全部功能而采用复杂的协议？OSI 参考模型功能虽然强大，但是否适应工业现场的通信环境？这些问题都是现场总线技术形成过程中必须考虑的重要问题。

那么我们来分析一下工业现场环境，工业生产现场存在大量传感、控制和执行等装置，它们通常相当零散地分布在一个较大范围内。对于底层通信网络来说，单个结点的信息量不大，信息传输的任务相对比较简单，但实时性的要求较高。如果采用 OSI 的全部七层参考模型，由于层间操作与转换的复杂性，势必增加网络接口的造价与时间的开销。因此，为了满足实时性要求，也为了降低成本，现场总线采用的通信模型大都在 OSI 模型的基础上进行了不同程度的简化。

典型的现场总线协议如图 3.2.1 第三列所示。它采用 OSI 模型中的三层：物理层、数据链路层和应用层，而省去了中间 3 至 6 层，考虑现场总线的通信特点。设置一个现场总线访问子层。它具有结构简单、执行协议直观、价格低廉等优点，也满足工业现场应用的性能要求。作为 OSI 模型的简化形式，其流量与差错控制在数据链路层中进行。总之，OSI 模型是现场总线技术的基础，现场总线参考模型既要遵循开放系统集成的原则，又要充分兼顾测控应用的特点和特殊要求。

自 80 年代末以来逐渐形成了几种有影响的现场总线技术，它们基本是以 OSI 作为框架，并根据行业的具体需要而加以改进的标准，从而获得了较为广泛的应用。下面将介绍几种主要的模型。

	OSI模型	现场总线协议	FF 总线模型	PROFIBUS	LonWorks
			用户层（程序）	用户接口	
7	应用层	应用层	信息规范子层 FMS 访问子层 FAS	或 应用层接口	应用层
6	表示层		隐去第 3 至 6 层	隐去第 3 至 6 层	表示层
5	会话层				会话层
4	传输层				传输层
3	网络层	总线访问子层			网络层
2	数据链路层	数据链路层	数据链路层	数据链路层	数据链路层
1	物理层	物理层	物理层	物理层	物理层

图 3.2.1　OSI 与部分现场总线通信模型的对应关系

3.2.1　基金会现场总线通信模型

基金会现场总线（FF，Foundation Fieldbus）是在过程自动化领域得到广泛支持，具有良好发展前景的技术。其前身是以美国 Fisher-Rosemount 为首的 80 多家公司制定的 ISP 协议和以 Honeywell 为首的 150 余家公司制定的 World FIP

协议。模型结构如图 3.2.1 第 4 列所示，它以 ISO/OSI 模型为基础，取其物理层、数据链路层、应用层为 FF 通信模型的相应层次，隐去了 3 至 6 层。应用层有两个子层：现场总线访问子层 FAS 和现场总线信息规范子层 FMS，并将从数据链路到 FAS，FMS 的全部功能集成为通信栈。FAS 的基本功能是确定数据访问的关系模型和规范，根据不同要求采用不同的数据访问工作模式。FMS 的基本功能是面向应用服务，生成规范的应用协议数据。这两个子层的任务是完成一个进程应用到另外一个进程应用的描述，实现应用进程之间的通信，提供应用接口的标准操作。为了实现网络管理和系统管理，还在应用层上增加了用户层。用户层主要针对自动化测控应用的需要，定义了信息存取的统一规范，采用设备描述语言规定了通用的功能模块集。

基金会现场总线分低速 H1 和高速 H2 两种通信速率。H1 的传输速率为 31.25kbps，通信距离可达 1900m，支持总线供电，支持本质安全防爆环境。H2 的传输距离可为 1Mbps 和 2.5Mbps 两种，其通信距离分别为 750m 和 500m。物理传输介质可支持双绞线、光缆和无线发射，协议符合 IEC1158-2 标准。其物理媒介的传输信号采用曼彻斯特编码。

3.2.2 PROFIBUS 通信模型

PROFIBUS 即 Process Fieldbus 的缩写，是德国国家标准 DIN19245 和欧洲标准 EN50170 的现场总线标准。本论文主要讨论的也就是这种总线标准。

它由 PROFIBUS-DP，PROFIBUS-FMS 和 PROFIBUS-PA 组成。DP 用于分散外设间的高速数据传输，适合于加工自动化领域的应用。FMS 即 Field Message Specification 的缩写，意为现场信息规范，适用纺织、可编程控制器、楼宇自动化等领域。PA 则是用于过程自动化的总线类型，遵从 IEC1158-2 标准。PROFIBUS 的传输速率为 9.6kbps~12Mbps，最大传输距离在 12Mbps 时为 100m，1.5Mbps 时为 400m，可用中继延长至 10km。其传输介质可以是双绞线，也可以是光缆。最多可挂接 127 个站点，可实现总线供电与本质安全防爆。

有关 PROFIBUS 的更多内容请参照后面的章节。

3.2.3 LonWorks 通信模型

LonWorks 是由美国 Echelon 公司推出并与摩托罗拉、东芝共同倡导，在 1990 年正式公布而形成的。它采用了 OSI 模型的全部七层通信协议，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，其通信速率从 300bps 至 1.5Mbps 不等，直接通信距离可达 2700m（78kbps，双绞线）。支持双绞线、同轴电缆、光纤、射频、红外线等多种通信介质，并开发了相应的本质安全防爆产品，被誉为通用控制网络。

LonWorks 技术所采用的 LonTalk 协议被封装在 Neuron 神经元芯片中。集成芯片中有三个 8 位 CPU，一个用于完成开放互连模型中第 1 和第 2 层的功能，称为媒体访问控制处理器，实现介质访问的控制与处理；第二个用于完成第 3~6 层的功能，称为网络处理器，进行网络变量的寻址、处理、背景诊断、路径选

择、软件计时、网络管理，并负责网络通信控制，收发数据包等。第三个是应用处理器，执行操作系统服务与用户代码。芯片中还具有存储信息缓冲区，以实现 CPU 之间的信息传递，并作为网络缓冲区和应用缓冲区。

LonWorks 已被广泛应用在楼宇自动化、家庭自动化、保安系统、办公设备、交通运输、工业过程控制等行业。

3.2.4 CAN 通信模型

CAN 是控制局域网络（Control Area Network）的简称，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。其总线规范已被 ISO 组织制定为国际标准，并广泛应用在离散控制领域。

CAN 协议仅采用了 OSI 模型中的两层，即物理层和数据链路层。物理层又分为物理信令（PLS Physical Signaling）、物理媒体附件（PMA，Physical Medium Attachment）和媒体接口（MDI，Medium Dependent Interface）三部分，完成电气连接、实现驱动器/接收器特性、定时、同步、位编码解码。数据链路层分为逻辑链路控制与媒体访问控制两部分，分别完成接收滤波、超载通知、恢复管理，以及应答、帧编码、数据封装拆装、媒体访问管理、出错检测等。

CAN 的信号传输采用短帧结构，因此传输时间短，受干扰的概率低。传输的介质为双绞线，通信速率最高可达 1Mbps/40m，直接传输距离最远可达 10km/5kbps。可挂接设备数最多可达 110 个。

3.2.5 HART 通信模型

HART 是 Highway Addressable Remote Transducer 的缩写。最早由 Rosemount 公司开发并得到 80 多家公司的支持，于 1993 年成立了 HART 通信基金会。这种开放通信协议的特点是在现有模拟信号传输线上实现数字信号通信，属于模拟系统向数字系统转变过程中的过渡性产品，因而在当前的过渡时期具有较强的竞争力，得到了较快发展。

HART 通信模型由三层组成：物理层、数据链路层和应用层。物理层采用 Bell 202 国际标准，数据链路层用于按 HART 通信协议规则建立 HART 信息格式。应用层的作用在于使 HART 指令付诸实现，即把通信状态转换为相应的信息。

HART 采用统一的设备描述语言 DDL。现场设备开发商用这种标准语言来描述设备特性，由 HART 基金会负责登记管理这些设备描述并把它们编为设备描述字典，主设备运用 DDL 技术来理解这些设备的特性参数而不必为此开发专用接口。HART 能利用总线供电，可满足本质安全防爆要求。

3.3 PROFIBUS 基本特性

PROFIBUS 可使分散式数字化控制器从现场底层到车间级网络化，该系统分为主站和从站。主站决定总线的数据通信，当主站得到总线控制权时，可主动向外界发送信息。从站为外围设备，没有总线控制权，仅对接收到的信息给

予确认或应主站的要求发回数据。由于从站只需总线协议的一小部分，所以实施起来特别经济。

3.3.1 传输技术

PROFIBUS 提供了三种数据传输类型：用于 DP 和 FMS 的 RS485 传输；用于 PA 的 IEC1158-2 传输；光纤。下面逐一介绍：

一、用于 DP/FMS 的 RS485 传输技术

由于 DP 与 FMS 系统使用了同样的传输技术和统一的总线访问协议，因而，这两套系统可在同一根电缆上同时操作。

RS-485 传输是 PROFIBUS 最常用的一种传输技术。这种技术通常称之为 H2。采用的电缆是屏蔽双绞铜线。

RS-485 传输技术基本特征：

网络拓扑：线性总线，两端有有源的总线终端电阻。

传输速率：9.6kbps 至 12Mbps

介质：屏蔽双绞电缆，也可取消屏蔽，取决于环境条件（EMC）。

站点数：每分段 32 个站（不带中继），可多到 127 个站（带中继）。

插头连接：最好使用 9 针 D 型插头。

二、用于 PA 的 IEC1158-2 传输技术

数据 IEC1158-2 的传输技术用于 PROFIBUS－PA，能满足化工和石油化工业的要求。它可保持其本质安全性，并通过总线对现场设备供电。

IEC1158-2 是一种位同步协议，可进行无电流的连续传输，通常称为 H1。

IEC1158-2 技术用于 PROFIBUS-PA，其传输以下列原理为依据：

- 每段只有一个电源作为供电装置。
- 当站收发信息时，不向总线供电。
- 每站现场设备所消耗的为常量稳态基本电流。
- 现场设备其作用如同无源的电流吸收装置。
- 主总线两端起无源终端线作用。
- 允许使用线性、树型和星型网络。
- 为提高可靠性，设计时可采用冗余的总线段。
- 为了调制的目的，假设每个总线段至少需用 10mA 基本电流才能使设备启动。通信信号的发生是通过发送设备的调制，从±9mA 到基本电流之间。

IEC1158-2 传输技术具有以下特性：

数据传输：数字式，位同步，曼彻斯特编码。

传输速率：31.25K bit /s，电压式。

数据可靠性：前同步信号,采用起始和终止限定符避免误差。

电缆：双绞线，屏蔽式或非屏蔽式。

远程电源供电：可选附件，通过数据线。

防爆型：能进行本质及非本质安全操作。

拓扑：线型或树型，或两者相结合。

站数：每段最多 32 个，总数最多为 126 个。

中继器：最多可扩展至 4 台。

三、光纤传输技术

PROFIBUS 系统在电磁干扰很大的环境下应用时，可使用光纤导体,以增加高速传输的距离。

可使用两种光纤导体，一是价格低廉的塑料纤维导体，供距离小于 50 米情况下使用，另一种是玻璃纤维导体，供距离小于 1 公里米情况下使用。

许多厂商提供专用总线插头可将 RS-485 信号转换成导体信号或将光纤导体信号转成 RS-485 信号，这样就为在同一系统上使用 RS485 和光纤传输技术提供了一套开关控制十分方便的方法。

3.3.2　协议结构

PROFIBUS 协议的结构以开放系统互联网络 OSI 为参考模型，如图 3.3.2.1 所示。

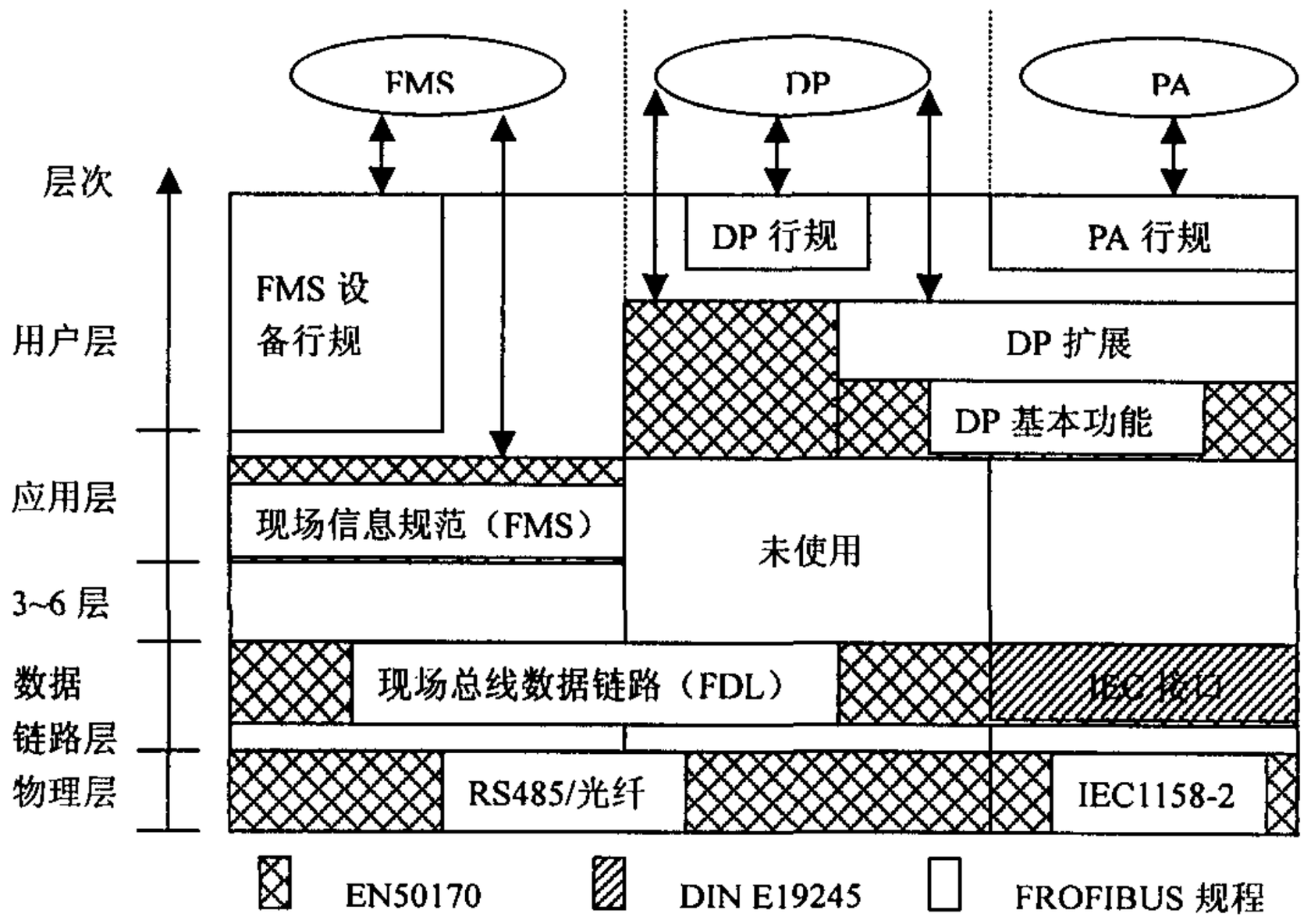


图 3.3.2.1　PROFIBUS 协议结构

PROFIBUS-DP 使用第 1 层，第 2 层及用户接口，第 3 层到第 7 层为加以描述，这种流体型结构确保了数据传输的快速和有效，直接数据链路（DDLM）提供易于进入第 2 层的用户接口，用户接口规定了用户及系统以及不同设备可

以调用的应用功能并详细说明了各种不同 PROFIBUS-DP 设备的设备行为，还提供了传输用的 RS-485 技术或光纤。

PROFIBUS-FMS 第 1，2 和 7 层均有定义，应用层包括现场总线信息规范（FMS，fieldbus message specification）和低层接口（LLI，lower layer interface）。FMS 包括了应用协议并向用户提供了可广泛选用的强有力的通信服务，LLI 协调了不同的通信关系并向 FMS 提供不依赖设备访问第 2 层。第 2 层现场总线数据链路（FDL，fieldbus data link）可完成总线访问控制和数据的可靠性，它还为 PROFIBUS-FMS 提供了 RS485 传输技术或光纤。

PROFIBUS-PA 数据传输采用扩展的“PROFIBUS-DP”协议，另外还使用了描述现场设备行为的行规，根据 IEC1158-2 标准，这种传输技术可确保其本质安全性并使现场设备通过总线供电。使用分段式耦合器 PROFIBUS-PA 设备能很方便地集成到 PROFIBUS-DP 网络。

PROFIBUS-DP 和 PROFIBUS-FMS 系统使用了同样的传输技术和统一的总线访问协议，因而这两套系统可在同一根电缆上同时操作。

3.3.3 总线存取协议

三种 PROFIBUS(DP、FMS、PA)均使用一致的总线存取协议。该协议是通过 OSI 参考模型第二层（数据链路层）来实现的。它包括了保证数据可靠性技术及传输协议和报文处理。

在 PROFIBUS 中，第二层称之为现场总线数据链路层（FDL）。介质存取控制（MAC，Medium Access Control）具体控制数据传输的程序，MAC 必须确保在任何一个时刻只有一个站点发送数据。

PROFIBUS 协议的设计要满足介质控制的两个基本要求：

- 在复杂的自动化系统（主站）间的通信，必须保证在确切限定的时间间隔中，任何一个站点要有足够的时间来完成通信任务。
- 在复杂的程序控制器和简单的 I/O 设备（从站）间通信，应尽可能快速又简单地完成数据的实时传输。

因此，PROFIBUS 总线存取协议，主站之间采用令牌传送方式，主站与从站之间采用主从方式。

令牌传递程序保证每个主站在一个确切规定的时间内得到总线存取权（令牌）。在 PROFIBUS 中，令牌传递仅在各主站之间进行。

主站得到总线存取令牌时可与从站通信。每个主站均可向从站发送或读取信息。因此，可能有以下三种系统配置：

- 纯主-从系统
- 纯主-主系统
- 混合系统

以一个由 3 个主站，7 个从站构成的 PROFIBUS 系统为例。3 个主站之间构成令牌逻辑环。当某主站得到令牌报文后，该主站可在一定时间内执行主站工作。在这段时间内，它可依照主-从通信关系表与所有从站通信，也可依照主

-主通信关系表与所有主站通信。

在总线系统初建时，主站介质存取控制 MAC 的任务是制定总线上的站点分配并建立逻辑环。在总线运行期间，断电或损坏的主站必须从环中排除，新上电的主站必须加入逻辑环。

第二层的另一重要工作任务是保证数据的可靠性。PROFIBUS 第二层的数据结构格式可保证数据的高度完整性。

PROFIBUS 在第二层按照非连接的模式操作，除提供点对点逻辑数据传输外，还提供多点通信，其中包括广播及选择广播功能。

在 PROFIBUS-FMS，DP 和 PA 中使用了第 2 层服务的不同子集，参考表 3.3.3.1，这项服务称为上层协议通过第 2 层的服务存取点（SAPS）。在 PROFIBUS-FMS 中，这些服务存取点用来建立逻辑通信地址的关系表；在 PROFIBUS-DP 和 PA 中，每个 SAP 点都赋有一个明确的功能。在各主站和从站当中，可同时存在多个服务存取点，服务存取点又有源 SSAP 和目标 DSAP 之分。

表 3.3.3.1　PROFIBUS 数据链路层的服务

服务	功能	DP	PA	FMS
SDA	发送数据要应答	无	无	有
SRD	发送和请求回答的数据	有	有	有
SDN	发送数据不需应答	有	有	有
CSRD	循环性发送和请求回答的数据	无	无	有

3.4 PROFIBUS-DP

PROFIBUS-DP 用于现场层的高速数据传送。主站周期地读取从站的输入信息并周期地向从站发送输出信息。总线循环时间必须要比主站程序循环时间短。除周期性用户数据传输外，PROFIBUS-DP 还提供智能化设备所需的非周期性通信以进行组态、诊断和报警处理。

传输技术：RS-485 双绞线、双线电缆或光缆。波特率从 9.6kbps 到 12Mbps。

总线存取：各主站间令牌传递，主站与从站间为主-从传送。支持单主或多主系统。总线上最多站点（主-从设备）数为 126。

通信：点对点（用户数据传送）或广播（控制指令）。循环主-从用户数据传送和非循环主-主数据传送。

功能：DP 主站和 DP 从站间的循环用户有数据传送。各 DP 从站的动态激活和撤消。DP 从站组态的检查。强大的诊断功能，三级诊断诊断信息。输入或输出的同步。通过总线给 DP 从站赋予地址。通过总线对 DP 主站（DPM1）进行配置，每 DP 从站的输入和输出数据最大为 246 字节。

可靠性和保护机制：所有信息的传输按海明距离 HD=4 进行。DP 从站带看门狗定时器（Watchdog Timer）。对 DP 从站的输入/输出进行存取保护。DP

主站上带可变定时器的用户数据传送监视。

PROFIBUS-DP 基本特征

速率：在一个有着 32 个站点的分布系统中，PROFIBUS-DP 对所有站点传送 512 bps 输入和 512bps 输出，在 12Mbps 时只需 1 毫秒。

诊断功能：经过扩展的 PROFIBUS-DP 诊断能对故障进行快速定位。诊断信息在总线上传输并由主站采集。诊断信息分三级：

本站诊断操作：本站设备的一般操作状态，如温度过高、压力过低。

模块诊断操作：一个站点的某具体 I/O 模块故障。

通过诊断操作：一个单独输入/输出位的故障。

PROFIBUS-DP 允许构成单主站或多主站系统。在同一总线上 最多可连接 126 个站点。系统配置的描述包括：站数、站地址、输入/输出地址、输入/输出数据格式、诊断信息格式及所使用的总线参数。每个 PROFIBUS-DP 系统可包括以下三种同类型设备：

一级 DP 主站（DPM1）：一级 DP 主站是中央控制器，它在预定的周期内与分散的站（如 DP 从站）交换信息。例如 PC。

二级 DP 主站（DPM2）：二级 DP 主站是编程器、组态设备或操作面板，在 DP 系统组态操作时使用，完成系统操作和监视目的。

DP 从站：DP 从站是进行输入和输出信息采集和发送的外围设备（I/O 设备、驱动器、HMI、阀门等）。

单主站系统即在总线系统的运行阶段，只有一个活动主站。

多主站系统是总线上连有多个主站，这些主站与各自从站构成相互独立的子系统。每个子系统包括一个 DPM1、指定的若干从站及可能的 DPM2 设备。任何一个主站均可读取 DP 从站的输入/输出映像，但只有一个 DP 主站允许对 DP 从站写入数据。

系统行为

系统行为主要取决于 DPM1 的操作状态，这此状态由本地或总线的配置设备所控制。主要有以下三种状态：

停止：在这种状态下，DPM1 和 DP 从站之间没有数据传输。

清除：在这种状态下，DPM1 读取 DP 从站的输入信息并使输出信息保持在故障安全状态。

运行：在这种状态下，DPM1 处于数据传输阶段,循环数据通信时，DPM1 从 DP 站读取输入信息并向从站写入输出信息。

DPM1 设备在一个预先设定的时间间隔内，以有选择的广播方式将其本地状态周期性地发送到每一个有关的 DP 从站。

如果在 DPM1 的数据传输阶段中发生错误，DPM1 将所有有关的 DP 从站的输出数据立即转入清除状态，而 DP 从站将不再发送用户数据。在此之后，DPM1 转入清除状态。

DPM1 和 DP 从站间的循环数据传输

DPM1 和相关 DP 从站之间的用户数据传输是由 DPM1 按照确定的递归顺

序自动进行。在对总线系统进行组态时，用户对 DP 从站与 DPM1 的关系做出规定，确定哪些 DP 从站被纳入信息交换的循环周期，哪些被排斥在外。

DMP1 和 DP 从站之间的数据传送分三个阶段：参数设定、组态及数据交换。在参数设定阶段，每个从站将自己的实际组态数据与从 DPM1 接受到的组态数据进行比较。只有当实际数据与所需的组态数据相匹配时，DP 从站才进入用户数据传输阶段。因此，设备类型、数据格式、长度以及输入输出数量必须与实际组态一致。

DPM1 和系统组态设备间的循环数据传输

除主-从功能外，PROFIBUS-DP 允许主-主之间的数据通信，这些功能使组态和诊断设备通过总线对系统进行组态。

同步和锁定模式

除 DPM1 设备自动执行的用户数据循环传输外，DP 主站设备也可向单独的 DP 从站、一组从站或全体从站同时发送控制命令。这些命令通过有选择的广播命令发送的。使用这一功能将打开 DP 从站的同步及锁定模式，用于 DP 从站的事件控制同步。

主站发送同步命令后，所选的从站进入同步模式。在这种模式中，所编址的从站输出数据锁定在当前状态下。在这之后的用户数据传输周期中，从站存储接收到输出的数据，但它的输出状态保持不变；当接收到下一同步命令时，所存储的输出数据才发送到外围设备上。用户可通过非同步命令退出同步模式。

锁定控制命令使得编址的从站进入锁定模式。锁定模式将从站的输入数据锁定在当前状态下，直到主站发送下一个锁定命令时才可以更新。用户可以通过非锁定命令退出锁模式。

保护机制

对 DP 主站 DPM1 使用数据控制定时器对从站的数据传输进行监视。每个从站都采用独立的控制定时器。在规定的监视间隔时间中，如数据传输发生差错，定时器就会超时。一旦发生超时，用户就会得到这个信息。如果错误自动反应功能“使能”，DPM1 将脱离操作状态，并将所有关联从站的输出置于故障安全状态，并进入清除状态。

电子设备数据文件（GSD）

为了将不同厂家生产的 PROFIBUS 产品集成在一起，生产厂家必须以 GSD 文件（电子设备数据库文件）方式将这些品的功能参数（如 I/O 点数、诊断信息、波特率、时间监视等）。标准的 GSD 数据将通信扩大到操作员控制级。使用根据 GSD 所作的组态工具可将不同厂商生产的设备集成在同一总线系统中。

GSD 文件可分为三个部分：

总规范：包括了生产厂商和设备名称、硬件和软件版本、波特率、监视时间间隔、总线插头指定信号。

与 DP 有关的规范：包括适用于主站的各项参数，如允许从站个数、上装/下装能力。

与 DP 从站有关的规范：包括了与从站有关的一切规范，如输入/输出通道

数、类型、诊断数据等。

PROFIBUS-DP 行规

PROFIBUS-DP 协议明确规定了用户数据怎样在总线各站之间传递，但用户数据的含义是在 PROFIBUS 行规中具体说明的。另外，行规还具体规定了 PROFIBUS-DP 如何用于应用领域。使用行规可使不同厂商所生产的不同设备互换使用，而工厂操作人员毋须关心两者之间的差异。因为与应用有关的含义在行规中均作了精确的规定说明。下面是 PROFIBUS-DP 行规，括弧中数字是文件编号：

NC / RC 行规（3.052）
编码器行规（3.062）
变速传动行规（3.071）
操作员控制和过程监视行规（HMI）

3.5 PROFIBUS-PA

PROFIBUS-PA 适用于 PROFIBUS 的过程自动化。PA 将自动化系统和过程控制系统与压力、湿度和液位变送器等现场设备连接起来，PA 可用来替代 4—20mA 的模拟技术。PROFIBUS-PA 具有如下特性：

适合过程自动化应用的行规使不同厂家生产的现场设备具有互换性。
增加和去除总线站点，即使在本质安全地区也不会影响到其它站。
在过程自动化的 PROFIBUS-PA 段与制造业自动化的 PROFIBUS-DP 总线段之间通过耦合器连接，并使可实现两段间的透明通信。
使用与 IEC1158-2 技术相同的双绞线完成远程供电和数据传送。
在潜在的爆炸危险区可使用防爆型“本质安全”或“非本质安全”。

PROFIBUS-PA 传输协议

PROFIBUS-PA 采用 PROFIBUS-DP 的基本功能来传送测量值和状态。并用扩展的 PROFIBUS-DP 功能来制订制现场设备的参数和进行设备操作。PA 第一层采用 IEC1158-2 技术，第二层和第一层之间的在 DIN19245 系列标准的第四部分作了规定。

PROFIBUS-PA 设备行规

PROFIBUS-PA 行规保证了不同厂商所生产的现场设备的互换性和互操作性，它是 PROFIBUS-PA 的一个组成部分。PA 行规的任务是选用各种类型现场设备真正需要通信的功能，并提供这些设备功能和设备行为的一切必要规格。目前，PA 行规已对所有通用的测量变送器和其它选择的一些设备类型作了具体规定，这些设备如：

测压力、液位、温度和流量的变送器
数字量输入和输出
模拟量输入和输出
阀门
定位器

3.6 PROFIBUS-FMS

PROFIBUS－FMS 的设计旨在解决车间监控级通信。在这一层，可编程序控制器之间需要比现场层更大量的数据传送，但通信的实时性要求低于现场层。

PROFIBUS-FMS 应用层

应用层提供了供用户使用的通信服务。这些服务包括访问变量、程序传递、事件控制等。PROFIBUS-FMS 应用层包括下列两部分：

现场总线住处规范（Fieldbus Message Specification，FMS）：描述了通信对象和应用服务。

低层接口（Lower Layer Interface，LLI）：FMS 服务到第二层的接口。

PROFIBUS-FMS 通信模型

PROFIBUS-FMS 利用通信关系将分散的过程统一到一个共用的过程中。在应用过程中，可用来通信的那部分现场设备称虚拟设备 VFD（Virtual field Device）。在实际现场设备与 VFD 之间设立一个通信关系表。通信关系表是 VFD 通信变量的集合，如零件数、故障率、停机时间等。VFD 通信关系表完成对实际现场设备的通信。

通信对象与通信字典（OD）

FMS 面向对象通信，它确认 5 种静态通信对象：简单变量、数组（一系列相同类型的简单变量）、记录（一系列不同类型的简单变量）、域和事件，还确认 2 种动态通信对象：程序调用和变量表（一系列简单变量、数组或记录）。

每个 FMS 设备的所有通信对象都填入对象字典（OD）。对简单设备，OD 可以预定义，对复杂设备，OD 可以本地或远程通过组态加到设备中去。静态通信对象进入静态对象字典，动态通通信对象进入动态通信字典。每个对象均有一个唯一的索引，为避免非授权存取，每个通信对象可先用存取保护。

ROFIBUS-FMS 服务

FMS 服务项目是 ISO 9506 制造信息规范 MMS （Manufacturing Message Specification）服务项目的子集。这些现场总线应用中已被优化，而且还加上了通信提出的广泛需求，服务项目的选用取决于特定的应用，具体的应用领域在 FMS 行规中规定。

低层接口（LLI）

第七层到第二层映射由 LLI 来解决，其主要任务包括数据流控制和联接监视。用户通过称之为通信关系的逻辑通道与其他应用过程进行通信。VMS 设备的全部通信关系都列入通信关系表 CRL（Communication Relationship List）。每个通信关系通过通信索引（CREF）来查找，CRL 中包含了 CREF 和第二层及 LLI 地址间的关系。

网络管理

FMS 还提供网络管理功能，有由现场总线管理层七层来实现。其主要功能有：上、下关系管理、配置管理、故障管理等。

PROFIBUS-FMS 行规

FMS 提供了范围广泛的功能来保证它的普遍应用。在不同的应用领域中，具体需要的功能范围必须与具体应用要求相适应。设备的功能必须结合应用来定义。这些适应性定义称之为行规。行规提供了设备的可互换性，保证不同厂商生产的设备具有相同的通信功能。 FMS 对行规做了如下规定（括号中的数字是文件编号）：

控制间的通信（3.002）
楼宇自动化（3.011）
低压开关设备（3.032）

3.7 互联网对现场总线技术的影响

互联网作为当代社会的信息高速通道，把大量局域网连接成广域网，对社会发展产生了重要影响。而现场总线技术作为一种实现自控设备间数字通信与控制网络互联的新技术，其发展趋势明显受到互联网技术的影响。

在现场总线产生初期，人们把主要注意力集中在满足控制的实时性、工业环境的抗干扰以及总线供电等控制网络特定条件下的需要。那时的现场总线传输速率大都较低，加上以太网采用载波监听多路访问的媒体访问控制方式，其通信的非确定性使人们一直认为它不适合于在控制网络中使用。随着技术的发展，现场设备对通信性能的要求提高，原有的现场总线技术已难以满足应用需求，而互联网由于技术成熟、性价比高等原因渐渐渗入控制网络领域。

现场总线控制网络位于企业信息网络的底层，其根本任务是要完成生产现场的测量控制，提供生产过程与设备的各种信息。从网络结构与企业信息集成的应用需求来看，企业要把管理、决策、市场信息和生产控制信息结合起来，把各种应用协调成一个整体，实现产品开发、生产加工、原料供应与产品存储、市场信息、企业管理、决策等过程的一体化解决方案，就需要把现场总线控制网络与企业内部网 Intranet、互联网 Internet 连接成一个整体。

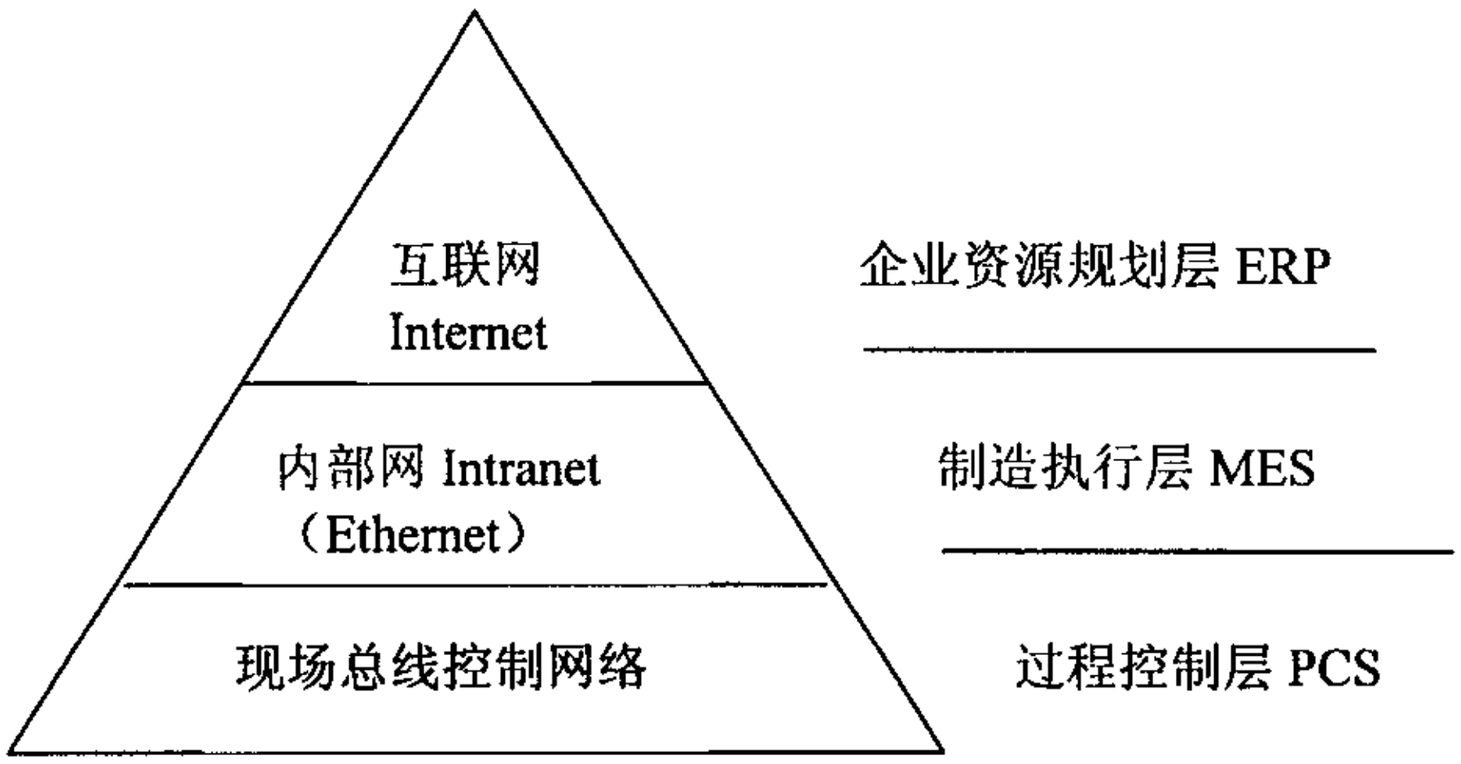


图 3.7.1 企业网络系统的层次结构

图 3.7.1 所示为企业网络系统的层次结构。一般可按功能把它划为三层：底层为完成生产现场测量控制功能的过程控制层 PCS（Process Control System）；最上层为企业资源规划层 ERP（Enterprise Resource Planning）；而传统概念上的监控、管理、调度等多项功能都被包罗在中间的制造执行层 MES（Manufacturing Execution System）。ERP 与 MES 层大多采用以太网技术构成网络，它们之间的网络集成与信息交换得到了较好解决，与外界互联网之间的信息交换也相对比较容易。

由于生产现场自控设备的种类繁多，测控设备间通信技术发展的相对滞后，使得在现场总线控制网络所处的过程控制层内部实现信息交换的难度较大。由于各种总线采用的网络协议和介质各不相同，不同标准的总线设备之间实现互连互操作存在很多障碍。而在一体化解决方案中，需要调用和设置许多该层的参数，互联网技术渗入到现场总线网络，无疑有助于实现层内与层间的信息集成。控制网络与互联网的结合拓宽了测量控制系统的范围与视野，为实现跨地区的远程控制与远程故障诊断创造了条件。我们可以在千里之外查询生产现场的运行状态；方便地实现偏远地区生产设备的无人看守；远程诊断设备故障等等。这些在控制网络与互联网的结合下都将成为可能。

通信非确定性问题

通信非确定性是互联网技术进入控制领域的最大障碍。现场总线网络不同于普通数据网络的最大特点在于它必须满足控制对实时性的要求。实时控制往往要求对某些变量进行准确的定时刷新，但由于以太网采用带冲突检测的载波监听多路访问的媒体访问控制方式，一条总线上挂接的多个节点采用平等竞争的方式争用总线。当节点要求发送数据时，首先监听总线是否空闲，如果空闲则发送数据，若总线忙则继续监听，直到总线空闲后再发送数据。即使如此也还会出现几个节点同时发送数据而冲突的可能性，因此传统以太网技术难以满足控制系统要求准确定时通信的要求，一直被称为非确定性网络。

正是快速以太网与交换式以太网技术的发展，给解决通信的非确定性带来了希望，使这一应用成为可能。目前以太网的通信速率一再提高，在相同通信量的条件下，通信速率的提高意味着网络负荷的减轻，而减轻网络负荷则意味着提高网络通信的确定性。

在全双工交换式以太网上，交换机将网络切分为多个网段，交换机之间通过主干网络相连。在网络分配合理的情况下，由于网段上多数的数据不需要经过主干网传输，而只是在本地网络传输，因此不占用其它网段的带宽，从而降低了所有网段和主干网络的负荷。

随着技术的发展，各现场总线相继推出了基于互联网技术的新一代现场总线技术和产品，它们在具体实施上有如下相似之处：

- 物理介质采用标准以太网连线
- 使用标准以太网连接设备
- 采用 IEEE 802.3 物理层和数据链路层标准、TCP/IP 协议组

- 兼容上一代现场总线系统甚至 DCS 系统
- 将传统的三层网络模型简化为两层甚至一层

PROFInet

针对工业应用需求，将原有 PROFIBUS 与互联网技术结合，形成了名为 PROFInet 的网络方案

PROFInet 主要包含三方面的技术：

- 基于组件对象模型（COM）的分布式自动化系统
- 规定了 PROFIBUS 和标准以太网之间的开放、透明通信
- 提供了一个独立于制造商，包括设备层和系统层的系统模型。

PROFInet 的基础是组件技术。在 PROFInet 中，每个设备都被看作一个具有 COM（*Component Object Module*，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 接口来调用设备功能。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。

PROFInet 采用标准 TCP/IP 以太网作为连接介质，采用标准 TCP/UDP/IP 协议加上应用层的 RPC/DCOM 来完成节点之间的通信和网络寻址。它可以同时挂接传统 PROFIBUS 系统和新型的智能现场设备。现有的 PROFIBUS 网段可以通过一个代理设备连接到 PROFInet 网络当中，使整套 PROFIBUS 设备和协议能够原封不动地在 PROFInet 中使用。传统的 PROFIBUS 设备可通过代理与 COM 对象进行通信，并通过 OLE 自动化接口实现 COM 对象之间的调用。

总之，互联网技术已深深影响了控制网络通信技术的发展，我国在开发自己的现场总线技术与产品时应充分注意到这一技术发展趋势。但也应看到，控制网络通信有其自身的特点，并非是照搬互联网技术可以替代的，需要发展适合应用需求的工业数据通信与网络技术。

4 SINEC-H1 高速工业局域网的分析与设计

SINEC-H1 是西门子 S5 系列可编程控制器的高速工业网络，其传输速度高达 10Mbps。它兼有工业控制局域网与办公自动化网的特点，主要用于区间级、单元级和设备级，实现管理、监控及控制功能。SINEC-H1 以“以太网协议”为基础建立，因此又被称为工业以太网，它与西门子近年推出的以 PROFIBUS 协议为基础的 SINEC-L2 网共同构成 S5 系列互联通信最主要的网络。

4.1 SINEC-H1 网的发展及特点

SIEMENS 公司的 S5U 系列的可编程控制器所采用的通信技术常用 3 种通信方式：星形点对点通信、低速总线型局部网络（SINEC-L2）L2 网，高速工业局部网（SINEC-H1）H1 网。

点对点通信是用于两个控制器之间的串行数据通信。控制器可以是可编程控制器（SIMATIC S5 系列）或外设（例如打印机）等。在 SIMATIC S5U 系列的点对点通信是通信处理器CP524和CP525组件来实现的一条计算机对计算机通信链路。其标准通信控制协议是 3964R。借助特殊的驱动器还能提供其他通信控制协议，从而使 SIMATIC 控制器能通过该链与其他厂商生产的控制器通信。

SIEMENS 公司采用主-从方式构成了适用于 S5U 系列可编程控制器的 SINEC-L1 局部网络。它适用于传输信息量不大，对速度要求不高的工业场合。可编程控制器分别为网络中的终端（或称节点），整个 SINEC-L2 网允许有 31 个节点（包括主站节点）。网络中最长的传输距离为 50km，2 个节点之间的最长传输距离为 4km，最大传输波特率为 9.6K 波特，每次传输最大的信息量为 64 个字节。在该网络中只能有一个主站，其余为从站。作为主站的可编程控制器必须采用CP530通信处理器组件与网络中的带电缆的总线端子BT777连接进网，而从站的可编程控制器则可通过编程接口或 CP530 组件与总线端子 BT777 连网。

随着工业上发展的需要，原有的 SINEC-L1 局部网的传输速度已不能适应需要。SINEC-H1 网为过程自动化提供了一个功能强大的通信工具，它是一个总线型网络系统，除了可与 SIEMENS S5 系列可编程控制器相连外，还能与 SICOMP（自动控制用计算机系统）、SINUMERIC（数控系统）和 SIROTEC（机器人）等自动化系统连网通信，其它系统也能借助接口组件与 SINEC-H1 连接。

表 4.1.1 给出了 SINEC-H1 网的协议模型，它是以 IEEE802.3 以太网标准为基础设计的局域网，采用 CSMA/CD(载波监听多路访问/冲突监测)访问技术，使用 SINEC H1-TF 和 SINEC H1-MAP 协议。图 4.1.1 所示为 IEEE802 的协议标准。

SINEC-H1 网是一种适于中、小规模的工业局域网，为过程自动化提供了一个功能强大的通用通信工具，它是一个总线型网络系统。为不同厂家不同产品间的互连和互操作提供了一种标准平台和接口，它几乎可以连接所有的自动

化设备和过程控制单元。

表 4.1.1 SINEC-H1 网络协议模型

ISO 层次	名　称	应　　用		
7	应用层	文件传送与存取	工厂自动化	虚拟终端
6	表示层			
5	会话层			
4	传输层	ISO DIS8073		
3	网络层	无效		
2b	数　据	IEEE802.2,逻辑链路控制(LLC)		
2a	链路层	IEEE802.3,介质访问控制(MAC), CSMA/CD		
1	物理层	IEEE802.3		

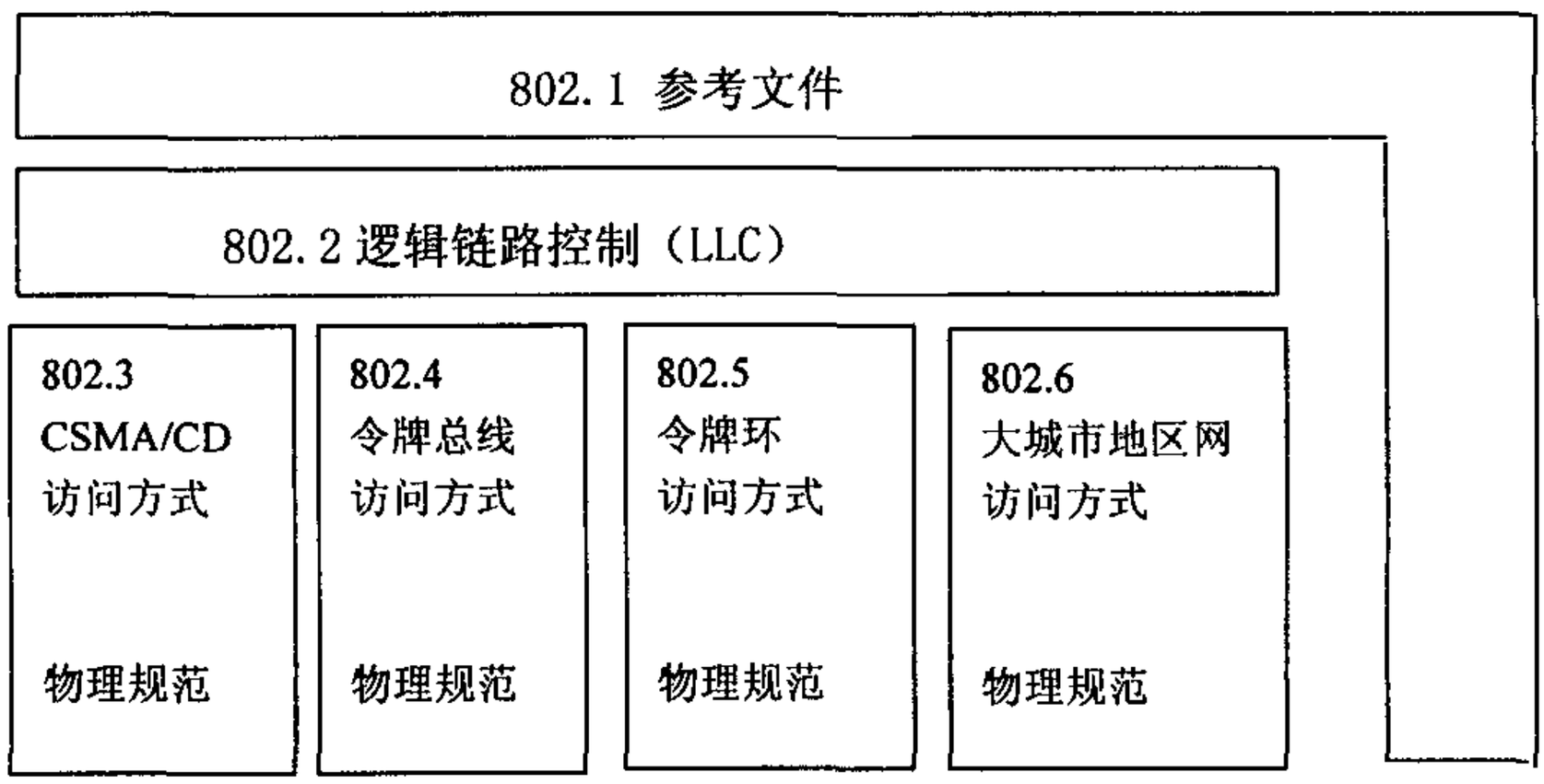


图 4.1.1 IEEE802 标准

与传统星形结构相比，总线型网络系统体现了很大的优越性，特别是在连接大而复杂的通信系统时，更具有以下特点：

- 低成本电缆,系统中各站点之间通信仅使用一条公共数据总线即可；
- 易扩展，要扩展站点不需要增加硬件接口就可以挂到总线网；
- 站点间通信自由，在总线网系统中，站点之相间互自由通信；
- 速度快，SINEC-H1 网采用了以太网作为总线型网的标准，传输速率达 10M 位/秒。

4.2 SINEC-H1 网的基本工作原理

站点与网的连接

SINEC-H1 局部网是用于可编程控制器等控制系统间高速大量的数据交换。站点上的可编程控制器 SIMATIC S5-115U、135U、155U 等通过通信处理器和一个传输器及电缆连到各段形成总线。

通信处理器有多个与用户程序的接口(多页地址)，其中每个都是相互独立的。所用的每个接口必须在启动程序中初始化。通信作业请求通过调用定义了接口号和作业号的数据处理单元传送到通信处理器。通信处理器一次可以处理多至 64 个作业(包括 32 个通信连接)。

通道上的数据交换

通信处理器在它有数据要传送时，主动地存取通道。网络中的每个站不断地在总线上“监听”，以找出它自己所需的数据，并接收它。数据只在通道不忙时被传送。两个站点若要同时发送数据，就将导致“数据冲突”。这种“冲突”会被检测到，而新的数据发送则将在一个随机时间间隔后才开始，该机间隔是通信处理器内部产生的。

在用户程序中用前述的数据处理单元来启动一次数据传送。可用的作业请求有：发送/接收（SEND/RECEIVE），写（WRITE），读（READ）。这些作业均可以各种传输方式（单工，半双工，全双工）传输，并且在直接/多播通信中有多种优先级。

传输方式

- 单工方式：数据只以一个方向传送，传送由主动可编程控制器调用“SEND”单元开始，被（从）动方可编程控制器调用“RECEIVE”功能单元开始来接收数据。
- 半双工方式：在“READ”作业请求时，用“FETCH”单元来读取数据。主动方的可编程控制器调用“FETCH”单元来发送要读数据的信息，从动方的可编程控制器调用“FETCH”功能来响应。
- 全双工方式：该方式只当通信双方都能主动发送或从动地接收数据时方能进行。此时，“SEND”和“RECEIVE”数据处理单元在两端都调用。

通信连接类型

- 直接通信连接，它是指两个站点的一般通信。从结构上来看，可以把它想象成一根电缆（而这不是物理意义上的电缆）。这就是有时称它虚拟通信连接的道理。直接通信连接的建立时间按不同的优先级而不同。对优先级 PRI00、PRI01 和 PRI02，在通信处理器 CP 组件从“STOP”状态变到“RUN”后立即建立；对优先级 PRI03 和 PRI04，在用户请求它时建立。该通信连接是在 CP 初始化定义在通信连接块中的。一般来说，SIMATICS5 可编程控制器之间的通信连接是根据接口号和作业号自动生成。主动方建立通信连接，并由被动方确认它。
- 多播通信连接，它是用于传送不要应答的、时间要求高的数据。这种

通信连接通常即不要确认连接是否建立，也不要确认数据是否被接收。它可以使一个站点的数据发送到一个特别的节点组。用户最多可以定义 64 个这样的多播组。当这样的组仅有两个站点时，称为数据通信连接。当该组包括有所有站点时称为“广播通信连接”方式。

优先级

- PRI00：中断驱动的快件服务。建立一个永久的带有静态数据缓冲区的通信连接，数据根据优先发送，且数据到达接收器时，就产生一个中断。
- PRI01：非中断驱动的快件服务。建立一个永久的带有静态数据缓冲区的通信连接，数据按优先级发送。
- PRI02：具有永久通信连接的一般服务。所需的数据缓冲器仅在作业处理期间动态建立。
- PRI03：根据请求而建立的一般服务。否则拆除通信连接和缓冲区直到数据被传送时才被建立，通信连接保持到用户在用户程序中调用“RESET”数据处理单元清除它为止。
- PRI04：根据请求而建立。否则拆除通信连接的一般服务。在这种优先级下，通信连接和数据缓冲区都是在数据传送时才建立，在传送过后，通信连接被立即拆除。

4.3 SINEC-H1 网络的使用

SINEC- H1 局部网上用于数据传送的作业有 3 种类型：SEND/RECEIVE（发送/接收）、WRITE（写数据）和 READ（读数据）。用户程序需要调用“SEND”、“RECEIVE”、“SYNCHRON”等 DHB 来完成这些作业，“RESET”功能可用来清除通信连接。有关 DHB 的详细说明请参照第 2 章。

- SEND/RECEIVE 作业：在 SEND/RECEIVE 作业的情况下，主动站点发送数据，被动站点接收数据。传送通过调用直接发送（SENDDIRECT）方式下的“SEND”处理单元来启动。
- WRITE 作业：当“WRITE”作业请求被发出时，主动站点发送数据，被动站点接收这些数据。与 SEND/RECEIVE 作业不同的是，数据源和目的地均是主动站定义的。“WRITE”请求只能服务于 PRI02 的优先级别。“WRITE”作业请求是通过调用直接方式下的 SEND 数据处理单元发出的。
- READ 作业：当 READ 作业请求被发出时（由主动站点发出），被动站点就发送数据，而主动站点接收它们。与 WRITE 作业一样，主动站点规定了数据源和目的地。READ 请求也只能被服务于 PRI02 优先级，READ 请求是通过调用“FETCH”数据处理单元发出的。
- RESET 作业：在应用程序中调用了数据处理单元时，就启动了一个 RESET。RESET 可以清除有相应的接口号和作业号“虚拟”通信连接。RESET 功能不该用于数据保文、多播、广播通信连接，因为此时它的

服务是没有实际意义的。

在使用前必须对通信处理器初始化，初始化包括有关每个通信连接的本地和全局的信息（通信连接块）以及通用参数（初始化块），另有一个用于系统范围内标识。

- 系统标识块：系统标识块用来提供一组统一的系统范围内的标识以及有关通信组件的类别标志，包括组件的固化软件的修改版本号，所有的存储器子组件的型号。最重要的参数是 CP 组件的基本接口地址和它的以太网地址（通道上的物理地址）。
- 初始化块：固化软件仅在通信处理开始工作时才读取初始化块中的参数。CP 组件自动生成初始化块，且只在特除情况下才需修改。这一信息块也包括有关 CP 组件的多播组信息。多播组是在通信连接块初始化时自动生成的，可以在初始化块中看到，但不能被修改。
- 通信连接块：通信连接块包含有一个通信连接的本地和全局的参数。它必须在每个通信连接的本地和远地的通信处理器中被定义。在通信双方的 CP 中其规范指标必须相同，因为 CP 是按这块中的信息生成直接的或多播的通信连接。通信连接的类型、作业类型及优先级也是定义在通信连接块中的。

4.4 组态（Configuration）及其软件

组态是工业网络中的一个重要概念。依据现场级设备的规格、使用的网络协议以及传输数据量的大小和速度的不同，需要预先对通信模板进行一些常规参数的设定，使之能正常运作，这就是组态（Configuration）。

4.4.1 组态软件功能分析

组态软件正在代替各种计算机语言的软件开发，其优点有：提高了系统的成功率和可靠性，这些组态软件大都是有专业软件公司开发，经过正规严格的测试，结合了大量用户的现场使用经验；缩短了项目开发周期，避免了许多重复性开发工作如画图等，突出了系统集成思想。开发人员着重于系统的整体选型、构成使得项目易于维护，避免因开发人员变化而带来的烦恼；减少开发费用。工控组态软件将形成计算机控制系统的软件主导地位。

组态软件主要具有以下功能：

- 丰富的画面显示组态功能：组态软件提供给用户丰富方便的作图工具，因为大中型控制系统要有大量的图形画面，而这些图形画面对开发人员是费时费力的。因此，组态软件提供大量常用的工业设备图符、仪表图符等；提供趋势图、历史曲线图等。
- 较强的通信性能和良好的开放性：组态软件向下能与部分硬件通信，向上能与高层管理网联。开放性是指组态软件能与多种通信协议互连，支持多种硬件。
- 组态软件完善，功能多样：组态软件提供工业标准数学模型库和控制

功能库，满足用户所需的测控要求；组态软件对测控信息进行记录、存贮、显示、计算、分析、打印，界面操作灵活方便，数据考虑安全性。

- 测控点规模及性能价格比较好：测控点的管理数量是衡量组态软件的重要参数。大型测控点系统要求强大的图形工具、丰富的菜单命令、完善的测点管理。组态软件能够满足这方面的要求。

目前，世界上有多家公司推出自己的工业控制组态软件，如 Rockwell 公司的 Rsview，Wonderware 公司的 Intouch5.6 软件等。但考虑性能价格、工厂实际等诸多因素，我们选用了西门子公司的 SIMATIC WinCC。

4.4.2 SIMATIC WinCC 的功能

WinCC 代表 **Windows Control Center**(视窗控制中心)，它是结合 SIEMENS 公司在过程自动化领域中的先进技术和 Microsoft 的强大功能的产物，是用来处理生产和过程自动化中的图形显示和控制任务的系统。此系统提供了在工业上用于图形显示、信息、归档和报表的功能模块。其强大的驱动程序接口、快速图象更新和安全归档功能具有很高的可用性。同时，WinCC 为用户提供了基于开放式接口的解决方案，通过标准接口 ODBC 和 SQL 能够访问所集成的归档数据。具体地说，它具有如下常见系统特性：

PC 机为基础和标准的操作系统

- 可在所有奔腾处理器的标准 PC 机上运行
- 32 位软件基于 Microsoft Windows 95 和 Windows NT 标准操作系统
- 可直接使用 PC 机提供的硬件和软件产品（例如 LAN 网卡）

具有 SCADA 功能（开放的系统内核）

- 图形系统：用于自由地组态画面，并完全通过图形对象（WinCC 图形，Windows，OLE，OCX 对象）进行操作。
- 报警信息系统：记录和存储事件并予以显示，操作简便符合德国 DIN19235 标准；可自由选择信息分类，信息显示和报表。信息系统用于监控生产过程事件、来自自动化级的事件以及 WinCC 系统事件，并进行处理。报警事件可触发指定的动作。
- 变量存档（标签归档）：接收、记录和压缩测量值如曲线和图表显示及进一步的编辑功能。
- 用户档案库：用于存储有关用户数据记录，如：数据管理及配方参数。
- 报表系统：用户自由选择一定的报表格式，按时间顺序或者事件触发来对信息操作、归档当前数据，进行用户报表输出。WinCC 提供了一套集成的报表系统，能方便的将过程中录入的数据输出。
- 处理功能：用 ANSI-C 句法原理编辑组态图形对象的动作，该编辑通过系统内部 C 编译器执行。
- 标准接口：通过 ODBC 和 SQL 访问用于组态和过程数据的 Sybase 数

据库。

- 编程接口：可在所有应用模块中使用，并提供便利的访问函数和数据功能。

强大的通信联网功能

在 WinCC 系统中，SIMATIC 提供了强大的网络功能，WinCC 可以通过 SINEC 网络、PROFIBUS 或串行通信方式与 SIMATIC S5/S7 交换数据，最多可接 1024 个节点，传输距离最长可达 23.8 km（光缆），最高速率为 10M 位/秒。

其通过 SINEC-H1 网与 S5 相连的结构如图 4.4.2.1 所示。

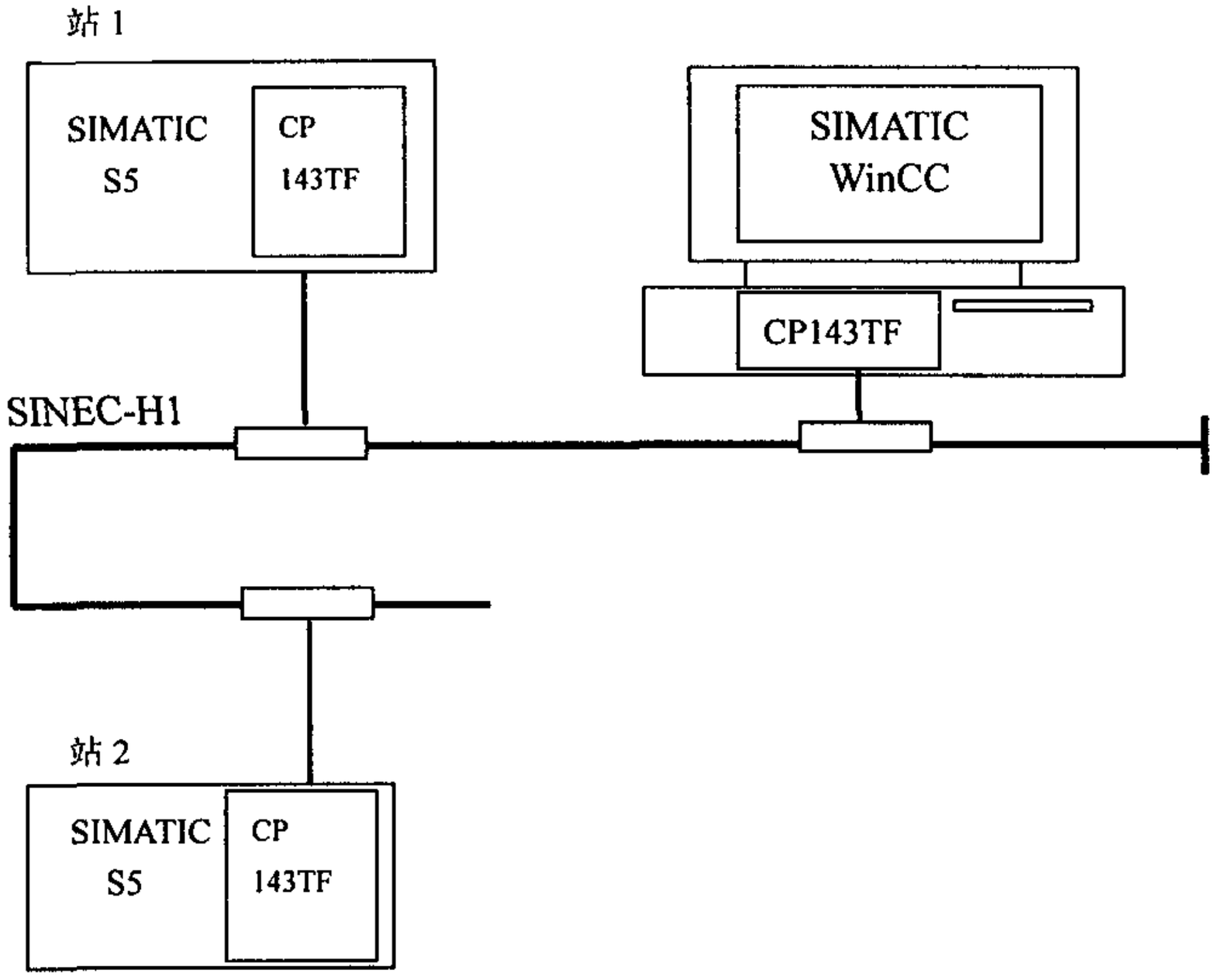


图 4.4.2.1　WinCC 与 S5 互连系统通信结构

综合考虑以上功能和优点和生产实际，选择 SIMATIC WinCC 作为该控制系统的软件开发工具。

4.4.3　CP143TF 的初始化编程（组态）

CP 的初始化,主要的参数有:

- 地址参数，包括主从机的 TSAPS 和从机的以太网地址。
- 作业类型，包括 SEND、RECEIVE、FETCH A/P。

● 传输参数。

用户程序结构系统识别参数 SYSID 和初始化块 INIT 主要是确定通信模块的类型、存贮器类型和容量，以及模块在 S5 机架上的外设地址和模块在网络中的以太地址。CP143TF 用户程序的主要内容在数据连接块。每个 CP143TF 可建立几十个个固定的数据连接块（优先级 0，1，2），同时还可处理一些暂态连接（优先级 3,4），但固定连接和暂态连接总数不得超过 64 个（同时限制固定连接不超过 32 个）。在每个数据连接块中主要是确定通信任务的类型、数据连接的方式以及连接类型和优先级。现分述如下。

任务的类型

任务的类型与 S5 中的标准功能块的类型相对应。它指的是该通信任务是发送数据，还是接收数据或是取数据。在一个数据连接块中最多允许有 4 个任务存在，但 CP143TF 处理任务的总数不得超过 64 个。

数据连接方式

CP143TF 的数据连接方式有 5 种，即：单向连接；带紧急数据服务的单向连接；半双向连接；双向连接；带紧急数据服务的双向连接。

单向连接在每个数据块中只能安排一个任务项，发送数据或接收数据，两者不能兼有。

半双向连接是相对于读数据通信而言的。读方先发一个请求电报，响应方则以数据电报返回。即数据可双向传送，但只有一方为主动。半双向连接在每个数据连接块中也只能安排一个任务项 FETCH（取操作），FETCH 有主动和被动之分。

双向连接不但数据可双向传递，而且连接的双方都可以是主动方。双向连接在每个数据连接块内同时安排 SEND 和 RECEIVE 两个任务项。

带紧急数据服务的单向连接在每个数据连接块中可安排 3 个任务项，而带紧急数据服务的双向连接则可安排 4 个。

数据连接类型

CP143TF 的数据连接类型有虚电路连接、多目的发送、广播方式以及数据报方式，多目的发送和广播方式易于理解。虚电路连接是在两个工作站的传送服务访问点（TSAP，任务号和 CP143TF 页号的组合）之间建立的严格对应关系，也就是说在一个数据连接块中的远程服务访问点（REMOTE TSAP）要与对方的本地服务访问点（LOCAL TSAP）相对应。虚电路有很高的服务质量，具有检错、重发、流量控制等功能。数据报的优点是发送及时，缺点是没有检错和应答重发功能，对数据传送的质量不负责任。

数据连接的优先级

一共分为 5 个优先级，0 级最高，4 级最低。0 级和 1 级用于多目的发送、广播方式和数据报。0 级是带中断的紧急数据服务，1 级则是不带中断的紧急数据服务。2 级为一般的固定连接，诸如发送数据、接收数据以及读写操作。3 和 4 级为暂态连接，3 级连接的拆除要用 RESET 功能块，而 4 级连接执行一次后就自动拆除。

由于优先级不同，处理的时间和方法也不一样，因而高层次和低层次优先级的连接就不能放在一个数据连接块内。具体划分为两个层次，0, 1, 2 级为一个层次，3、4 级为另一个层次。结合上述分析，根据实际应用情况，就可以编制数据连接块了。

需要注意的是 SINEC-H1 的 S5 CPU 中的标准功能块任务参数只面向本地 CP143TF 中的数据连接块，只有数据连接块才是面向网络的。因而在编制程序时，要注意标准功能块和 CP143TF 的数据连接块的配合关系。另外，SINEC-H1 要用到的标准块的种类较多，应用较灵活，比如取（FETCH）、发送（SEND）、接收（RECEIVE）的使用也有全部和直接之分。

图 4.4.3.1 给出了 CP143TF 基本初始化的有关参数。

CP143TF 基本初始化参数	
SYSID 块参数：	以太网地址：080006010000H 基本接口号（SSNR）：12
INIT 块参数：	以太网地址：080006010000H
LINK 1~n 块参数：	**本地 PLC** SSNR：12　　A-NR：x 作业类型：　　主动/被动（A/P）：P **远程 PLC** 以太网地址：080006010000H SSNR：yy　　A-NR：x

图 4.4.3.1　CP143TF 基本初始化的有关参数

4.5 通信系统的软件设计

下面给出 CPU2（通用控制处理器）的有关通信程序。其程序结构如图 4.5.1 所示。

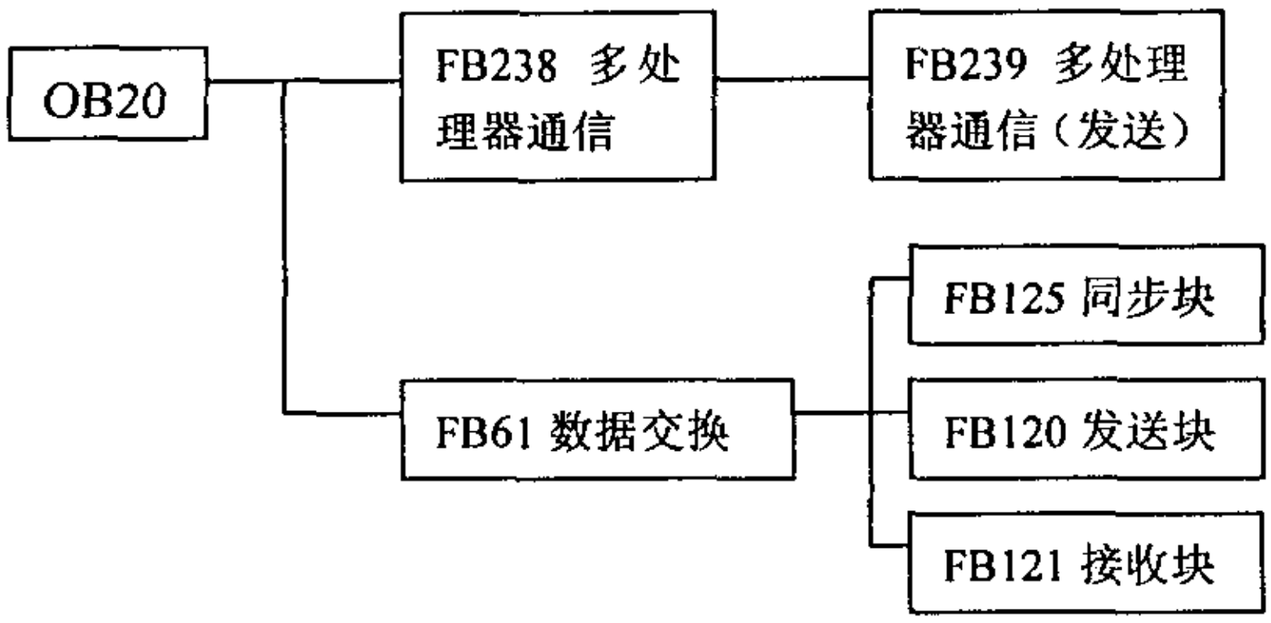


图 4.5.1　冷启动通信程序结构简图

```
OB 20
Segment   1
        :AN   F    22.7
        :S    F    22.6
        :S    F    22.4
        :S    F    22.0          重启标志位
        :C    DB    3            DB3中的数据传送给F标志字
        :L    DW    1
        :T    FW   25
        :L    DW    2
        :T    FW   27
        :L    DW    3
        :T    FW   29
        :***

Segment   2
        :O    F    26.5
        :O    F    26.6
        :JC   FB 238              多处理器通信
Name :MPC
XINI :      F    22.4
XEMP :      F    22.5
XSEN :      F    22.5
        :A    F    27.0
        :A    F    27.1
        :JC   FB   61             与通信模板的数据交换
```

```
Name :VMO-H
XNEU :      F     22.4
      :BE
```

FB 238

```
Segment   1
Name :MPC
Decl :XINI          I/Q/D/B/T/C: I   BI/BY/W/D: BI
Decl :XEMP          I/Q/D/B/T/C: I   BI/BY/W/D: BI
Decl :XSEN          I/Q/D/B/T/C: I   BI/BY/W/D: BI
      :C     DB 238
      :AN    =XINI
      :JC    =M001
      :L     DW    2                  初始化923C
      :T     FW 190
      :L     KB 190
      :JU    OB 200
      :L     FW 196                   条件码字输入数据块
      :T     DW   32
      :BEU
M001 :***
Segment   2
      :AN    =XEMP
      :JC    =M003
      :L     DL    1                  接收测试
      :T     FY 190
      :L     KB 190
      :JU    OB 205
      :L     KB 0                     检查条件码是否出错
      :L     FY 192
      :!=F
      :JC    =M001
      :T     DR   41
      :JU    =M003
M001 :L      FY 193
      :L     KB 0
      :!=F
```

```
      :JC   =M030
      :L    DL    1          接收
      :T    FY 190
M002 :L     KB 190
      :JU   OB 204
      :JM   =ERR
      :L    FY 193           检查是否还有接收容量
      :L    KB 0
      :>F
      :JC   =M002
      :JU   =M003
ERR :L     FY 192
      :T    DR   40
      :L    KB 1
      :T    DL   40
M003 :***

Segment   3
      :AN   =XSEN
      :BEC
      :L    FW 160
      :L    FW 162
      :OW
      :T    DW   45
      :L    DL    1          发送测试
      :T    FY 190
      :L    KB 190
      :JU   OB 203
      :L    KB 0             检查条件码是否出错
      :L    FY 192
      :!=F
      :JC   =M002
      :T    DR   42
      :BEU
M002 :L     FY 193           检查发送容量
      :L    DR   15
      :>=F
      :JC   =M003
      :BEU
```

```
M003 :***

Segment   4
        :L    DW    1
        :T    FW 190
        :L    DL   17
        :T    FY 192
        :L    DR   23
        :T    DR   43
        :L    DL   23
        :T    DR   44
        :L    DR   17
        :T    DR   46
        :JU   FB 239
Name :MPC-S1
M001 :BE

FB 239
Segment   1
Name :MPC-S1
        :L    KB 0
        :T    FY 102
        :L    DR   43
M001 :L    KB 0
        :<=F
        :JC   =WARN
        :L    DR   44              发送
        :T    FY 193
        :L    KB 190
        :JU   OB 202
        :L    FY 194               出错则转至错误处理程序
        :JM   =ERR
        :L    KB 1
        :T    FY 102
        :JP   =WARN                警告则转至警告处理程序
        :L    KB 0
        :T    FY 102
        :L    DR   44
        :I          1
```

```
      :T    DR   44
      :L    DR   43
      :D          1
      :T    DR   43
      :JU   =M001
WARN :AN    F   102.0
      :S    F   102.1
      :BEU
ERR :DO   DW   46
      :T    DR    0
      :BE
```

DB238

```
DW0:      KH = 0000;
DW1:      KY = 002,001;
DW2:      KY = 001,002;
DW15:     KY = 000,024;
DW17:     KY = 246,047;
DW20:     KY = 000,050;
DW21:     KY = 000,051;
DW23:     KY = 000,004;
DW24:
```

FB 61

```
Segment   1
Name :VMO-H
Decl :XNEU          I/Q/D/B/T/C: I   BI/BY/W/D: BI
      :C    DB   69
      :AN   =XNEU
      :JC   =M001
      :L    DR    1
      :T    FY    4
      :L    KB 0
      :T    FY    2
      :A    F     4.0
      :JC   FB 125                    同步块
Name :SYNCHRON
SSNR :      KY 0,12                   直接赋值SSNR=12
```

```
BLGR :      KY 0,5          帧大小256字节
PAFE :      FY   2          同步出错字
      :L    FY   2
      :T    DL   4
      :L    KB 0
      :T    DW   6
      :T    DD   7
      :T    DD  10
      :BEU
M001 :***

      Segment  2
            :L    DL   6
            :T    FY   2
            :JU   FB 120              发送块
      Name :SEND
      SSNR :      KY 0,12
      A-NR :      KY 0,0              SEND-ALL
      ANZW :       DW   7
      QTYP :      KS NN
      DBNR :       KY 0,0
      QANF :       KF +0
      QLAE :       KF +0
      PAFE :      FY   2
            :L    FY   2
            :T    DL   6
            :L    DR   6
            :T    FY   2
            :JU   FB 121              接收块
      Name :RECEIVE
      SSNR :      KY 0,12
      A-NR :      KY 0,0              RECEIVE-ALL
      ANZW :       DW  10
      ZTYP :      KS NN
      DBNR :       KY 0,0
      ZANF :       KF +0
      ZLAE :       KF +0
      PAFE :      FY   2
            :L    FY   2
```

```
        :T    DR    6
        :***
        :

Segment   3
        :C    DB    88              理论值
        :AN   D     43.0
        :C    DB    87              实际值
        :=    D     59.0
        :BE
```

DB69

DW0:　　KH = 0000;
DW1:　　KM = 00000000 00000001;
DW2:　　KH = 0000;
DW3:

5 SINEC-L2 现场级局域网的分析与设计

在工厂计算机控制系统的分层模型中，低三级为单元级、设备级、装置级。按照原现场总线的概念，这三级的通信任务，要由两级通信子网去完成。其中一级子网只负责控制器与传感器及执行器之间的通信，而二级子网只负责控制器与控制器、控制器与操作站之间的信息传送。然而新现场总线的概念则不同，它把这两级通信子网合二为一，单元级、设备级和装置级三级的通信任务全部由一级子网完成，这就要求新现场总线在存取控制方面独具特点，能最大限度发掘出工业局域网的通信潜能。

西门子公司实现 S5 系列互联的 SINEC-L2 网即是这种现场总线，它采用 PROFIBUS 协议，与 S7 系列的 PROFIBUS 现场总线相兼容。有关 PROFIBUS 的详细内容请参见第 3 章。

5.1 SINEC-L2 的特点

SINEC-L2 局域网的通信介质为屏蔽双绞线，采用分布式单段结构或者分布式多段结构。单段结构不用中继器，由一段总线组成，最多可接入 32 个站。若采用基带传输、RS485 总线标准，最远距离为 1200m；若采用调频传输，则可使最远距离达到 5km。在多段结构的 SINEC-L2 网中，每段最多可接入 32 个站，整个多段结构的站点总数不得超过 127 个，段与段之间要采用中继器连接，在任何两站之间不得超过 7 台中继器。

5.2 SINEC-L2 的存取控制方式

SINEC-L2 工业局域网采用令牌方式与主从方式相结合的存取控制方式。

令牌控制主站浮动

在 SINEC-L2 网中的站分为主动站与从动站两类。主动站共同控制 SINEC-L2 网访问权的分配，而从动站处于被动地位，只有当受到主动站要求时，才发送或接收数据。对于 L2 网而言，一般各种 S5 可编程控制器、联网的 PC 及编程器等都是主动站，而传感器、变送器、执行器等为从动站。

如图 5.2.1 所示，图中 PS 为前站地址，TS 为本站地址，NS 为下站地址。首先由 SINEC-L2 总线上的主动站组成逻辑环，让一个令牌在逻辑环中按一定方向依次流动。凡获得令牌的站也就获得了 SINEC-L2 网的访问权，并获得批准的令牌持有时间。在这段时间内，该主动站就成为整个 L2 网中的主站。这就是所谓的令牌控制主站浮动的含义。如果在整个 L2 网上有 M 个站，其中有 N 个主动站（N<M），那么将通过令牌控制使主站在这 N 个主动站中浮动，通常又把这种方式称为 N：M 方式。如果总线上有 N 个站，这 N 个站全是主动站，令牌将在这 N 个站中传递，这种方式称为 N：N 方式，可以将它视为 N：M 方式的特例。如果在总线上的全部 N 个站中只有一个主站，这时采用主从方式分配总线访问权，又称为 1：N 方式。

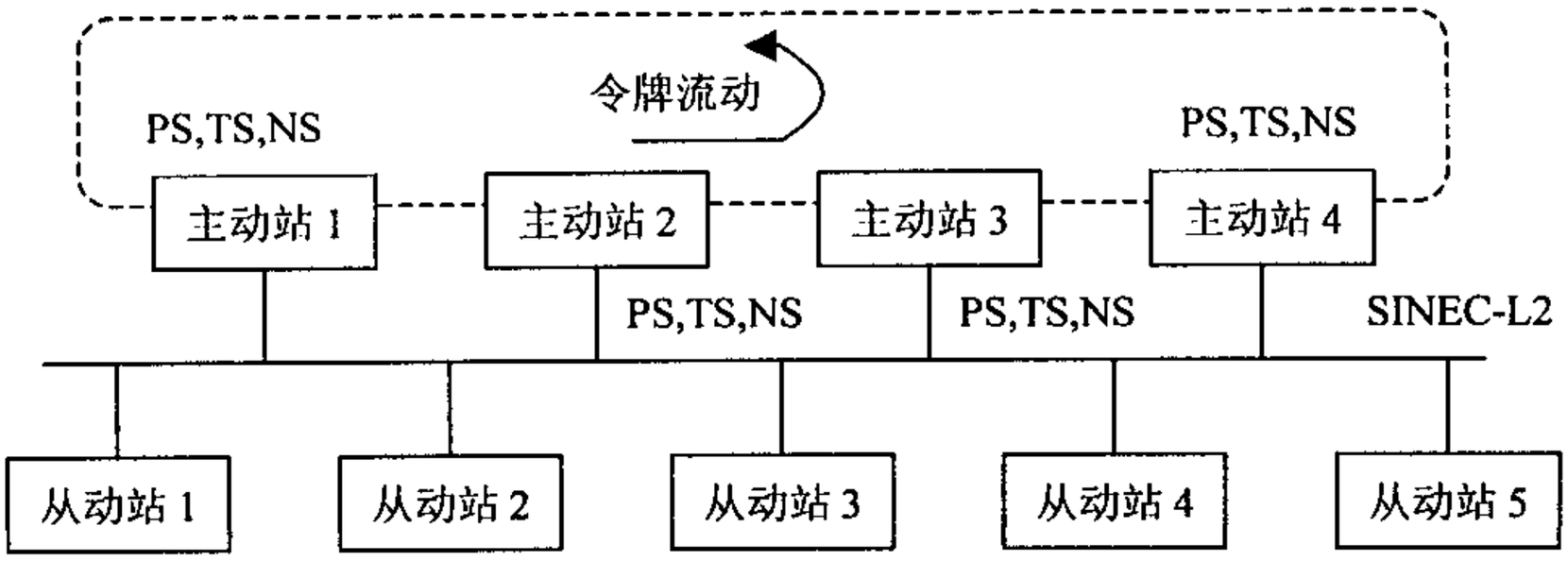


图 5.2.1 SINEC-L2 局域网中的令牌总线

主从方式按优先级调度

一旦一个主动站获得了令牌，这个站在一段时间内就成为了全网中唯一的主站。在这段时间内它按主从方式控制与管理网络，按优先级进行调度，需要完成三项任务：

- 进行逻辑环维护
- 向高优先级任务提供服务
- 向低优先级任务提供服务

FDL 接口的用户具有对两个服务优先级的选择，即低优先级与高优先级。一个站一旦获得了令牌，首先要进行逻辑环维护，这是每个主动站必须完成的任务，这段时间一般不计入令牌持有时间。然后处理所有高优先级任务，最后处理低优先级任务。高优先级任务总会得到服务，即使超出了令牌持有时间，也应把高优先级任务处理掉。在高优先级任务处理完之后，再根据令牌持有所剩时间对低优先级任务进行调度。

凡是由主动站用户提出的通信要求，用户应同时对其服务优先级进行选择。对于这一类由主动站用户随机提出来的任务，采用非周期发送请求方式传输数据。还有另一类通信任务是由用户预先在每个主动站中输入了一张轮询表（Polling list），该表由用户预先定义了此主动站在获得令牌后所有应当轮询的从动站及其某些其它主动站，并规定该主动站与轮询表中各站按照周期发送/请求方式进行数据传输。对于这种预先安排在轮询表中的任务，SINEC-L2 规定一律按低优先级任务调度。

对低优先级任务调度的安排是这样的：当处理完高优先级任务之后，如果剩有令牌持有时间，则先安排周期发送/请求任务，即轮询表规定的任务，按照轮询表规定的顺序，在令牌持有时间内，采用 CSRD 方式（周期发送/请求方式）向各站发送数据，并要求立即给予带数据的应答。

如果轮询表执行完后，令牌持有时间剩余部分还够处理一个低优先级非周期发送/请求任务，则执行之；若所剩时间不够，则在下次获得令牌并处理完高优先级任务后，再对低优先级任务处理。先处理上次留下来的低优先级非周期发送/请求任务，然后再执行轮询表。

如果轮询表较长，执行完整个轮询表将超出令牌持有时间，这时应当对轮询表进行分段处理。等到分段处理完成后，再安排对低优先级非周期发送/请求任务的处理。

非周期发送/请求与周期发送/请求

（1）非周期发送/请求

凡由某主动站的用户随机提出的通信请求，在该主动站获得令牌后，按非周期发送/请求方式进行数据传输。由于用户通信请求带有随机性，因此无周期性可言，这类任务被称为非周期发送/请求任务。它有三种工作方式：

- SDN：无应答发送数据，可把数据发到一个站或所有站（广播），但不需要应答。
- SDA：有应答发送数据，把数据发到一个站，要求立即应答。
- SRD：把数据发送到一个站，要求对方发回带数据的应答。

非周期发送/请求任务可以由用户为其选择高服务优先级或低服务优先级。

（2）周期发送/请求方式（轮询表方式）

在每个主动站中，用户预先定义一个轮询表，规定了在此主动站获得令牌后应询问的从动站及其它一些主动站。这些任务的预先安排的，不是用户随机提出的，而令牌周期循环，该主动站每获得令牌就有可能执行一遍，因此称为周期发送/请求任务，采用 CSRD 方式进行传输。

CSRD 方式即周期 SRD 方式，它指周期性地按轮询表向各站发送数据并要求立即给予带数据的应答。周期发送/请求任务按低优先级调度。

5.3 SINEC L2-DP 的数据传输方式

SINEC L2-DP 遵循 PROFIBUS-DP 协议，有关 PROFIBUS-DP 的详细内容参见第 3 章。它规定了四种数据传输方式，即：预组态连接与 DHB 结合的传输方式，对层 2 自由访问与 DHB 结合的传输方式，全局 I/O 传输方式以及周期 I/O 传输方式。下面分别予以分析。

5.3.1　预组态连接方式

预组态连接方式是指把预先已经组态好的 L2 网上可编程控制器互联与 DHB 数据管理功能块的调用结合起来实现 L2 网数据通信的一种数据传输方式。这种方式适合于在 SINEC-L2 工业局域网上的主动站之间，最大长度不超过 128 字节的相邻接数据帧的交换。

当采用预组态连接方式时，必须与 DHB 块相结合才能实现数据通信，必须把发送作业块与接收作业块按作业号分配给预组态连接。当建立缺省连接时

符合下列关系：

- 用发送作业号 X，向网上的站 X 发送数据
- 用接收作业号（100+X），从网上的站 X 接收数据
- 用本地的服务访问点 SAP（1+X），与网上的站 X 建立连接

预组态连接与 DHB 结合传送数据的过程为：

- 一旦启动，COM5430（CP5430 的组态工具）就在所有主动站之间自动建立起缺省连接（即预组态连接）。
- 在 SEND 的 FB 参数中，指定要发送的数据。
- 当 SEND 作业启动时，把这些参数送到 CP5430 的指定存储区或双口 RAM 中。
- CP5430 按 PROFIBUS 协议规定，在要发送的数据上加上协议数据单元后，按 SDA 发送/请求帧格式发送给网上预组态连接的对方站。
- 接收站的 CP5430 对收到的报文作应答并且通过对其作业状态字相应位置 1，使 SEND 作业结束。
- 接收站的 CP5430 向接收站的用户程序报告数据收完。
- RECEIVE 块启动，把接收到的数据从双口 RAM 中取出，放入由 RECEIVE 块 FB 参数指定的存储区中。

5.3.2 层 2 自由访问方式

ISO 提出的把所有通信功能组合在一起的 7 层体系结构中，第 2 层为数据链路层，它用于确保在数据链路上的可靠数据传输。采用 7 层模型，其通信速度较慢，对于工业局域网来说，较难满足实时性要求。如果不要这么多层，我们可以在 STEP5 用户程序上通过调用 DHB 功能块来直接访问第 2 层，要求第 2 层提供服务来实现 L2 网的数据通信。显然这样将大大加快通信速度，提高实时性，这就是所谓的层 2 自由访问方式。

采用层 2 自由访问方式意味着用户在 STEP5 程序中要请求（Request）第 2 层提供数据传输服务，并对来自第 2 层的确认（Confirmation）进行评判，而对方则应对 CP5430 收到报文时发出的指示（Indication）进行评判。

对层 2 的访问只能通过 LSAP（数据链路层服务访问点）进行，只能通过这些 SAP 请求 FDL 服务。因此在调用 DHB 时要为其分配一个 SAP 点。

层 2 自由访问也必须与 DHB 功能块调用结合起来才能实现 L2 网上的数据通信。层 2 自由访问方式适合于 SINEC-L2 网上主动站之间相邻接数据帧的传送，帧的最大长度为 246 个字节。

层 2 自由访问与 DHB 结合的数据传输过程为：

- 在对 CP5430 组态时，只指定本地参数（即本地 SSNR 及 A-NR），并给作业号分派一个 SAP 点。
- 把要发送的信息在发送缓冲区中预先准备好。它由报头与数据两部分组成，在报头中包括了目标地址（对方的站地址及 SAP 地址）以及 FDL 服务标识符。

- 当发送方的 SEND 作业启动时，把发送缓冲区中的报头与数据送给自己的 CP5430。
- 在报头信息的控制下，CP5430 建立起 PROFIBUS 报文，并把报文送到 SINEC-L2 网上。
- 依据所请求的 FDL 服务来处理数据传输。
- 在接收方，RECEIVE 块启动，可编程控制器从自己的 CP5430 的双口 RAM 中取走通信专用报头及数据，并把它们存入由 RECEIVE 块的 FB 参数指定的区域中。
- 用户程序对报头进行解读。

第 2 层提供的 FDL 服务除前面提到的 SDA、SDN 及 SRD 外，还有另外两种。

- RPL-UPD-S：用来把数据输入到发送缓冲区中，然后这些数据将被对方的 SRD 服务取走，最后清空发送缓冲区。
- RPL-UPD-M：与 RPL-UPD-S 服务功能相同，只不过当数据被对方 SRD 服务取走后原数据仍然保留在发送缓冲区中。

5.3.3 全局 I/O 方式

如果在多微机系统中建立一块每台微机都可以寻址访问的存储区，那么以此为中介，就可以实现多微机之间的通信。这块存储区称为共享存储区，这种通信的方式就称为共享存储区通信方式，该通信方式常用于并行总线的多微机系统。

这种通信方式也可用在串行总线系统中，只不过对共享存储区的结构要做些改变。假设一个局域网上有 N 个站，从每个站都划分出一块大小一样的存储区，那么对这块存储区而言，各站都可以寻址访问，于是它就成了共享存储区。在物理上要把这 N 块分散在各站的存储区合并是无法实现的，然而在逻辑上却完全可以把这 N 块存储区合并成大小与其中任何一块相等的存储区，这只需要局域网通过周期性的通信，使这 N 块存储区中存放的数据等值化。因此各站只要通过访问自己的那块存储区，也就实现了与其它站交换数据的目的。这就是所谓的串行共享存储区通信。

从本质上看，SINEC-L2 局域网采用的全局 I/O 方式就是一种串行共享存储区通信方式。这种方式要求 L2 网上以 S5 为端点的主动站都要划出一块大小相等的 I/O 区作为共享存储区使用。要能成为共享区必须由 L2 网通过等值化通信来实现，为此共享存储区采用信箱结构，如图 5.3.3.1 所示。每个站的共享区都设有一个发送信箱及（N－1）个接收信箱。

全局 I/O 方式通信的特点为：

- 各站均划出一块 I/O 区作为共享区用，此共享区映射到自己的 CP 上，称为 GO 区。
- GO 区的结构在图 5.3.3.1 中做了表示，采用信箱结构。图中“1#发”表示 1#站的发送信箱，“2#收”表示接收 2#站发送数据的存放处，其

它以此类推。等值化通信就是分别用 1#、2#、3#发送信箱内容更新 1#、2#、3#接收信箱内容，那么 3 个站中 3 个 GO 区的内容就等值化了。

- L2 局域网对 GO 区进行等值化通信采用的报文称为全局报文，也称 GP 字节。全局报文只包含那些变化了的 GO 区发送信箱的内容，采用广播方式通信。当某站广播 GP 字节时，L2 网上所有主动站 GO 区同号接收信箱都要接收下此广播的 GP 字节。全局报文自动具有高优先级，在 L2 网中优先传送。
- CP 刷新发送信箱可采用异步或同步方式，CP 把接收到的数据提交给主动站的 CPU 输入区也可采用异步或同步方式。
- 在 CP 组态时，设置 I/O 区与 CP 的 GO 区的映射关系。在图 5.3.3.1 中设 GO 区第一个字为 GPW30，如果在对 CP 组态时设定：CP1 中 QW55=GPW30，CP2 中 IW18=GPW30，CP3 中 IW10=GPW30，则由图可见，经过站 1，站 2，站 3 用户程序及全局 I/O 方式的通信作用，当站 1 的 FW18 变化时，1#的 QW55，2#的 QW3 以及 3#的 QW10 都将跟着变化。
- 全局 I/O 方式不适用于大批量的数据交换，因为它占用 I/O 区。一般用于站间单个字的数据通信，这种方式通信速度较快。

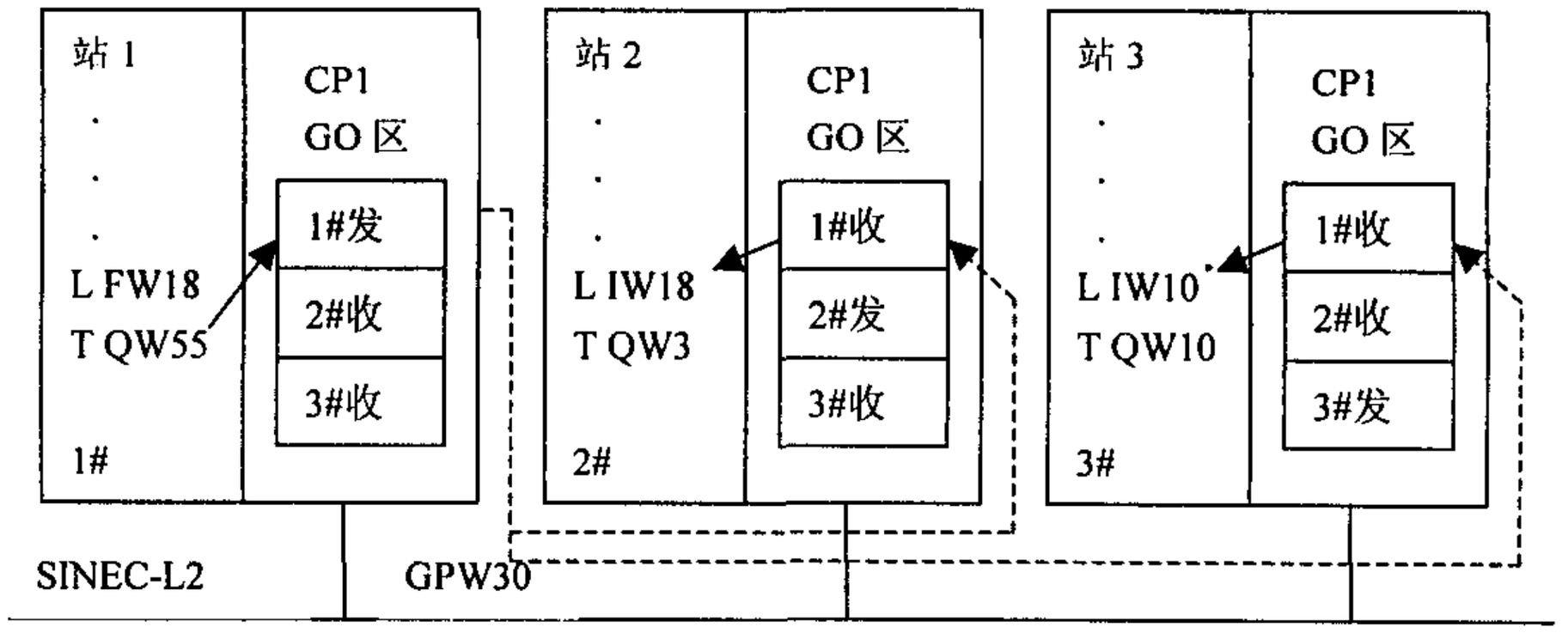


图 5.3.3.1　全局 I/O 方式共享区结构及通信原理

5.3.4　周期 I/O 方式

周期 I/O 方式适用于 S5 与它的现场设备之间的数据交换。由于现场设备都是些从动站，它们不具备对局域网访问的能力，因此必须由 L2 局域网上的主动站按主从方式，采用周期轮询，向从动站发送数据或者从从动站读取数据。由于这种方式从动站要占据主动站的一部分 I/O 区，而且数据通信周期性进行，

所以称为周期 I/O 方式。这种方式不适合传输大批量数据，因为它占用主动站 I/O 区，但其通信速度较快。

周期 I/O 方式既可采用异步方式刷新，也可采用同步方式刷新。所谓异步方式是指由主动站的 CP 来决定刷新时刻，与 STEP5 的控制程序无关。而同步方式是指要通过在 STEP5 用户程序中调用作业号为 210 的 SEND 块及作业号为 211 的接收块来决定刷新时刻。

周期 I/O 方式的数据传输过程为：

- 在对 CP 组态时，要把主动站的周期 I/O 分配给各从动站(即现场设备)。
- 主动站只要使用输出指令向周期 I/O 的输出区分派数据，就完成了向现场设备发送数据的任务。
- 主动站只要使用输入指令从周期 I/O 的输入区读取数据，就完成了从现场设备接收数据的任务。
- 在主动站所带的通信模板 CP 中建立了一个集中数据库，用于周期 I/O 方式通信。CP 采用异步方式或同步方式刷新这个数据库。它请求 SRD 服务，把周期 I/O 数据库全部输出区的数据发送给各从动站，并从各从动站读取数据存入周期 I/O 数据库的输入区。这样就保证了此数据库的实时性，以使主动站的 CPU 随时可以用输入/输出指令与其交换数据。周期 I/O 报文在 L2 网中具有低优先级。

5.4 STEP5 程序的编制

由于系统中有两块 CPU928，其中 CPU1 负责与工业以太网的级联与通信，而 CPU2 作为通用控制处理器，负责与现场设备、I/O 模块的通信。通过两个 CPU 之间的通信（由 FB238 实现多处理器间数据交换），CPU1 可及时获取现场设备的实际数据（例如进料流量、温度、张力等等），然后以一系列经典的工业控制算法，实现负反馈控制，使得实际值与理论值之间保持在一个可以容忍的误差范围之内。并实时地将数据传送给 H1 网，WinCC 则以图形界面的形式将数据显示在工控机上，实现集中监视和报警功能。如果检测到数据异常，超出了规定的安全极限，则转入异常处理程序。

由于只有一块通信模板，所以两块 CPU 需共享通信模板中的同一块存储区域。这就造成了一种潜在的危险，因为它们可能会在不恰当的时候复写同一地址的内容，从而导致数据的混乱。为了解决这个问题，STEP5 程序中引入了旗号（Semaphore）这个概念，旗号（0~31）是唯一的。当其中一块 CPU 要访问某一存储区时，必须设置相应的旗号，设置不成功则无权访问该存储区。当其对这一区域的数据存取结束后，必须释放此旗号，以使这一存储区可以被另一 CPU 访问。这就避免了数据误读误写的危险。在 STEP5 程序中，这种设置与释放旗号的操作分别由 SED 和 SEE 来实现。

综上所述，我们除了对 CP 的初始化组态之外，还必须分别在 CPU1 及 CPU2 编制用户程序。由于 CPU2 的部分程序在第 4 章已作了介绍，因此本节主要是关于 CPU1 用户程序的编制。其程序的主结构如图 5.4.1 所示。

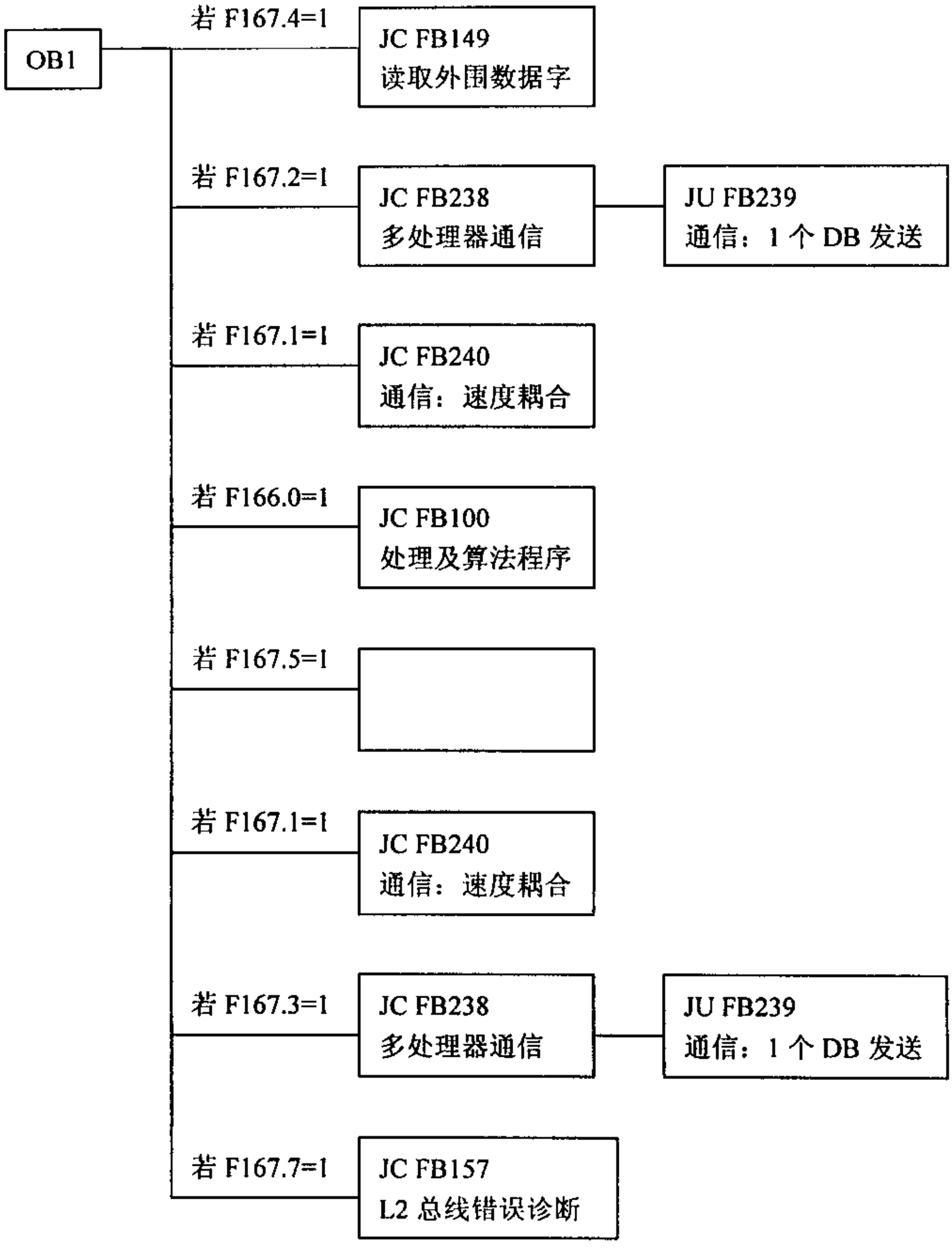


图 5.4.1 CPU1 用户程序主结构简图

部分程序如下：

```
OB 1
Segment   1
        :C     DB     3
        :L     DW     1              读入状态字
        :T     FW 166
        :***

Segment   2
        :A     F    167.4
        :JC    FB 149               读取外围数据字
Name :SHA<AO
        :A     F    167.2
        :JC    FB 238               多处理器通信
Name :MPC
XINI :       F    164.5
XEMP :       F    164.4
XSEN :       F    164.5
        :A     F    167.1
        :JC    FB 240               通信：速度耦合
Name :MPC<>S
EING :       F    164.4
        :***

Segment   3
        :A     F    166.0
        :JC    FB 100               处理及算法程序
Name :KAS-ORG
        :A     F    167.5
        :JC    FB 151               写入外围数据字
Name :SHA>AO
        :A     F    167.1
        :JC    FB 240               通信：速度耦合
Name :MPC<>S
EING :       F    164.5
        :A     F    167.3
        :JC    FB 238               多处理器通信
Name :MPC
```

```
XINI :      F   164.5
XEMP :      F   164.5
XSEN :      F   164.4
      :***

Segment   4
      :A    F   167.7
      :JC   FB 157                L2总线错误诊断
Name :DIA-L
      :BE
```

DB3

```
      DW1:        KM = 11001011 11111111;
      DW2:
```

FB 149

```
Segment   1
Name :SHA<AO
      :C    DB 151
      :L    PW 192
      :T    DW    2
      :L    PW 194
      :T    DW    3
      :L    PW 196
      :T    DW    4
      :L    PW 198
      :T    DW    5
      :L    PW 200
      :T    DW    6
      :L    PW 202
      :T    DW    7
      :L    PW 204
      :T    DW    8
      :L    PW 206
      :T    DW    9
      :BE
```

```
FB 240
Segment   1
Name :MPC<>S
Decl :EING          I/Q/D/B/T/C: I   BI/BY/W/D: BI
      :SED      30                  设置旗号
      :JZ   =M001
      :JU   =M002
M001 :BEU
M002 :***
Segment   2                         从共享区读取数据
      :C    DB 245
      :AN    =EING
      :JC   =M001
      :L    KH F280
      :LIR        1
      :T    DL    1
      :L    KH F281
      :LIR        1
      :T    DR    1
      :L    KH F282
      :LIR        1
      :T    DL    2
      :L    KH F283
      :LIR        1
      :T    DR    2
      :BEU
M001 :***

Segment   3                         向共享区写入数据
      :L    DL    9
      :L    KH F290
      :TIR        3
      :L    DR    9
      :L    KH F291
      :TIR        3
      :L    DL   10
      :L    KH F292
      :TIR        3
```

```
      :L    DR  10
      :L    KH F293
      :TIR       3
      :***
Segment  4
      :SEE       30              释放旗号
      :BE
```

FB 151

```
Segment  1
Name :SHA>AO
      :C    DB 151
      :L    DW  12
      :T    PW 192
      :L    DW  13
      :T    PW 194
      :L    DW  14
      :T    PW 196
      :L    DW  15
      :T    PW 198
      :L    DW  16
      :T    PW 200
      :L    DW  17
      :T    PW 202
      :L    DW  18
      :T    PW 204
      :L    DW  19
      :T    PW 206
      :BE
```

FB 157

```
Segment  1
Name :DIA-L
      :C    DB 246
      :L    KB 16
      :T    PY 255
      :L    KY 127,0
```

```
:T    PW 252
:L    PY 252
:T    DR  83
:L    PY 253
:T    DL  83
:BE
```

6　系统的可靠性研究及设计

作为一个现场总线构成的系统，其应用于高自动化程度、高产值、高复杂度的工业过程控制数据通信中，这些工作过程虽然各不相同，但都有下述的特点：一方面由于生产过程的高复杂度和高自动化程度，操作人员对自动控制系统的依赖性越来越大；另一方面，如果系统中出现故障，不但会破坏被控设备、危及操作人员的安全，而且仅仅短期停产造成的损失就会远远超过控制网络系统本身的价格。由此可见，工业过程控制对控制系统的可靠性提出了多方面的严格要求：系统必须保证能够长期连续地无故障运行，一旦发生故障，系统必须具有故障自动检测功能及安全保护功能。

6.1 可靠性的基本理论

可靠性是产品质量的指标，其定义为：产品在规定的条件下，规定的时间内，完成规定的能力。其中规定条件是指产品工作时所处的环境条件、维护条件、使用条件等，规定时间是指考察产品是否正常工作的起止时间，规定功能则是指产品应当实现的功能。

衡量可靠性的常用量化指标有：

- 可靠度

在国家标准中对可靠度的定义是：产品在规定的条件下和规定的时间内完成规定的概率。

设有 N_0 个同样的产品，在同样的条件下开始工作，从开始运行到时间 t 之间，有 $N_f(t)$个发生故障，$Ns(t)$个未发生故障，则其可靠度 $R(t)$可表示为：

$$R(t)=\frac{Ns(t)}{N_f(t)+Ns(t)}=\frac{Ns(t)}{N_0} \tag{6.1.1}$$

- 失效率

失效率是指系统运行到 t 时刻后的单位时间内发生故障的系统数与时刻 t 时完好的系统数之比。

N_0 个系统的可靠度为 $R(t)$，则从 t 时刻到 $t+\Delta t$ 时刻失效的系统系数为 $N_0\times[R(t)-R(t+\Delta t)]$，则在 t 时刻后单位时间的失效数为 $N_0\times[R(t)-R(t+\Delta t)]/\Delta t$，则在时刻 t 时完好的系统数为 $N_0\times R(t)$，将失效率记为 $\lambda(t)$，则有：

$$\lambda(t)=\frac{N_0\times\dfrac{R(t)-R(t+\Delta t)}{\Delta t}}{N_0\times R(t)}=\frac{R(t)-R(t+\Delta t)}{R(t)\times\Delta t} \tag{6.1.2}$$

将上式改写为微分形式，得到：

$$\lambda(t) = -\frac{1}{R(t)}\frac{dR(t)}{dt} \tag{6.1.3}$$

上式又可以写成：

$$\lambda(t)dt = -\frac{dR(t)}{R(t)} \tag{6.1.4}$$

$$\int \lambda(t)dt = -\ln R(t)\Big|_{1}^{R(t)} \tag{6.1.5}$$

对上式从 0 到 t 积分，得到：

λ(t)的单位是时间的倒数。对于产品而言，λ(t)与时间 t 的关系如图 6.1.1 所示，这就是著名的浴盆曲线。

即：

$$R(t) = {}_{e} - \int \lambda(t)dt \tag{6.1.6}$$

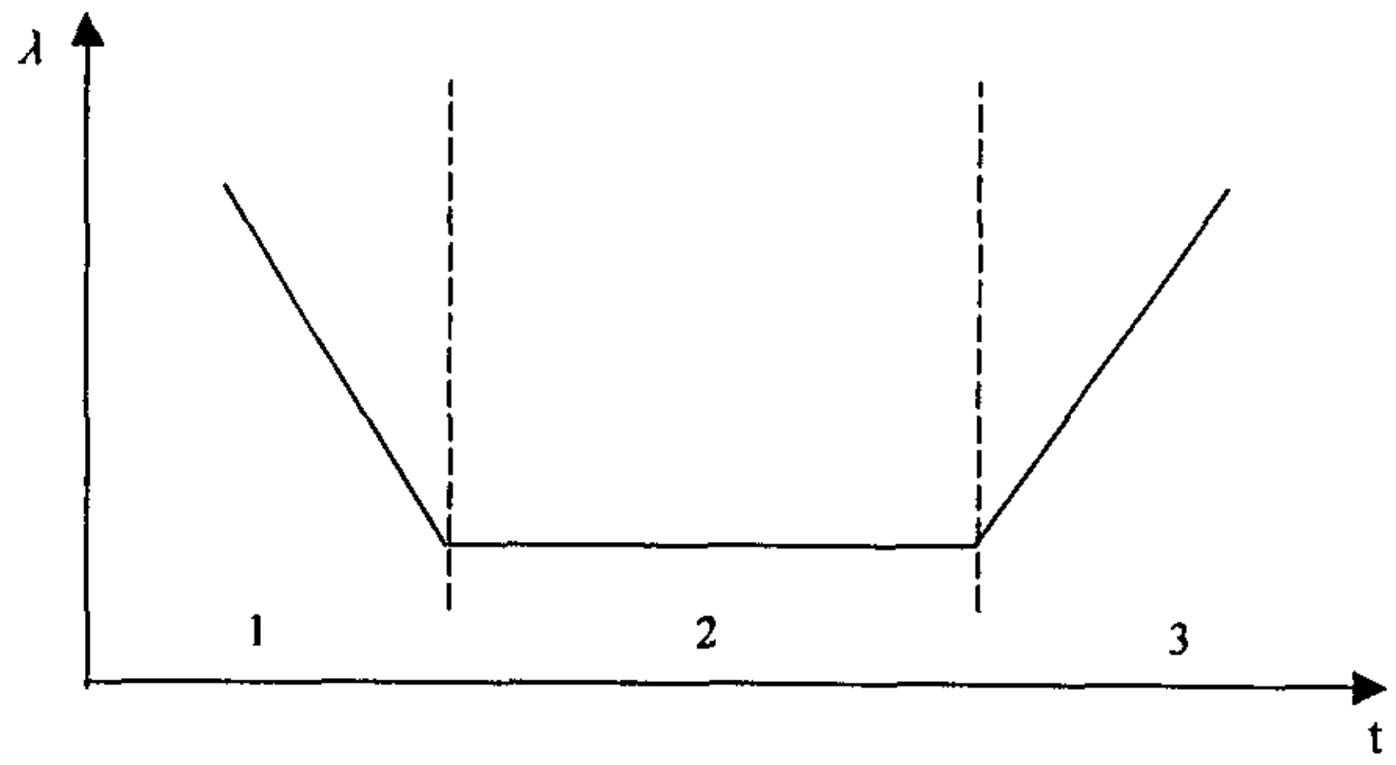


图 6.1.1 浴盆曲线

该曲线可分为三个部分，第一部分为早期失效期，这一时期内引起产品失效的主要原因是生产过程的缺陷，随着 t 时间的增加这种情况迅速减少；第二部分为偶然失效期，其中 λ(t)很低，并且几乎与时间 t 无关，这一时期也称为寿命期，它持续的时间很长；第三部分为耗损失效期，这一时期内产品已达到其寿命，失效率迅速上升。

通常情况下，一种产品经过适当的老化处理，可以很快地渡过早期失效期而进入偶然失效期，偶然失效期是一个长期稳定的过程。因此，在分析产品的

可靠性指标时，一般是指产品在偶然失效期内的可靠性。

产品的可靠性指标常用以下几种：

● 平均寿命与平均维修时间

根据可靠度的定义，如果一种产品在时刻 t 内正常工作的概率为 $R(t)$，则按照统计学理论，该产品的寿命的数学期望值亦即平均寿命 m 可表达为：

$$m = \int_0^{+\infty} R(t)dt \tag{6.1.7}$$

结合式(6.1.6)，得到：

$$m = \int_0^{+\infty} {}_e - \lambda t = \frac{1}{\lambda} \tag{6.1.8}$$

也就是说，产品的平均寿命是其失效率的倒数。

如果产品出现故障后无法修复，则其寿命 m 代表的是平均无故障时间 MTTF（Mean Time To Failure）；如果产品故障可以修复，则其寿命 m 代表的是平均故障间隔时间 MTBF（Mean Time Between Failure）。现场总线网络系统的故障均应是可以修复的，故在此将平均寿命统称为 MTBF。对可修复系统，还有一个重要的可靠性指标，即平均修复时间 MTTR（Mean Time To Repair）。

● 利用率

利用率是修复产品的一个可靠性指标，由下式定义：

$$A = \frac{MTBF}{MTBF + MTTR} \tag{6.1.9}$$

也就是说，利用率是产品正常工作的时间占总时间的比率。为提高利用率，一方面要尽量提高产品的 MTBF，另一方面还要努力减少产品的 MTTR。

6.2 系统的可靠性设计

在具体组网设计控制系统时，在可靠性方面需考虑以下几点原则：

● 提高系统各单元的 MTBF

在可靠性理论中，单元越简单，可靠性越高。现场总线控制系统（FCS）作为继集散控制系统（DCS）之后新一代控制系统，将全系统分为自律性极强的多个独立单元，每个单元比较简单，可靠性大为提高，并且某一部分发生故障，也不致导致影响整个系统。另外，结构上的分散也就意味着控制的分散、供电的分散、负荷的分散及干扰的分散，因此从根本上分散了影响可靠性的外部因素，从而能够保证系统达到很高的 MTBF。

● 降低系统各单元的 MTTR

本控制系统中采用模块结构设计，各个模块功能简单，易于维护，在发生故障时便于及时发现故障位置，迅速更换，有利于缩短系统的平均维修时间

MTTR，从而提高系统的利用率。

- 采用冗余与容错技术

容错技术的出发点是承认各单元发生故障的可能，进而设法保证即使某单元发生故障，系统仍能完成正常工作。为了使系统具有容错能力，必须在系统中增加适当的冗余单元，保证当某个单元发生故障时能由冗余单元接替其工作，原单元修复后再恢复出错前的状态。所以容错与冗余是同时使用的技术。

在集中式控制系统中，如果进行冗余容错必须对全系统进行冗余，这是很复杂而又很不经济的。而在分散式控制系统中，由于各单元的相对的相对独立和相对简化，使得冗余容错比较容易实现，同时还便于在冗余时突出重点，减少不必要的冗余，从而使系统更为经济实用。

在本现场总线控制系统中，采用了改进的分散结构，其性价比更优于集散控制系统。同时，在其自身的设计中，又采用了冗余措施和容错技术。其平均无故障运行时间（MTBF）超过两万小时，而平均修复时间（MTTR）则少于 20 分钟。

另外，操作管理站设计了两台监控计算机，互为备用地执行监控任务，这称之为双机系统。双机系统的工作方式一般分为备份工作方式和双工工作方式两种。

在备份工作方式中，一台作为主机投入系统运行，另一台作为备份机也处于通电工作状态，作为系统的热备份机。当主机出现故障时，专用程序切换装置便自动地把备份机切入系统运行，承担起主机的任务。而故障排除后，原主机则转为备份机，处于待命状态。

在双工工作方式中，两台主机并行工作，同步执行同一任务，并比较两机执行结果。如果比较相同，则表明正常工作；否则，再重复执行，再校验两机结果。以排除随机故障干扰。若经几次重复执行与核对，两机结果仍然不相同，则启动故障诊断程序，将其中一台故障机切离系统，让另一台主机继续执行。

在本系统，使用WinCC冗余软件包，使WinCC同时运行在两个站上，这种配置的优点是WinCC冗余系统的存档匹配功能保证了数据的完整性。这种匹配在象化纤这样连续质量控制的场合是必须的。另外，WinCC的冗余结构保证了生产过程管理和操作的可靠性。在通常情况下，两个WinCC站完全地并行操作。如果两个WinCC站中的一台故障，另一台接管信息存档和过程数据存档。当故障修复再次启动时，两个站又有了同样的数据。

结论

在工业自动化领域中，随着自动化程度的提高和对控制系统实时性、可靠性要求的提高，集中控制系统已不能满足用户的需求，现在很多控制系统都采用集散计算机控制，它是将管理计算机、过程控制计算机、数据通信系统、显示操作系统及各种智能仪表通过网络有机地结合起来，各设备之间通过网络来交换数据和传送指令，功能强大、组态灵活、扩展性和重构性好、可靠性和可维护性高。但同时这也对网络的通信功能提出了更高的要求，要实现数据通信和互操作，这无疑需要强有力的软、硬件支持。此外，在特殊的工业环境下，如强电磁干扰、有毒有害气体及严重污染场合都要求有网络组件。根据实际课题的需要，作者选用了西门子公司的 SINEC 网络产品，采用 SINEC-H1、SINEC-L2 及 S5-135U 远程 I/O 系统三级子网组构了整个工业控制通信网络，实现了工业现场设备的通信。另外，采用 WinCC 组态软件对系统组态，从而解决了在操作站级和管理级的人机界面问题。

通信系统的软件是系统的核心。软件的设计以硬件为基础，体现出通信系统的实时性、自主性、灵活性和可靠性。在本系统的设计和分析中，从软件的功能分析、概要设计、详细设计和运行调试过程，我们始终遵循了软件工程化的原则，取得了令人满意的结果。

结合盐城八菱化纤厂的课题，作者设计完成了后纺车间基于 SIMATIC SINEC 网络的通信系统。主要工作为：

- 完成了可编程控制器的通信程序的设计。
- 完成西门子 SINEC-H1 网总体框架设计。
- 完成西门子 SINEC-L2 网总体框架设计。
- 完成了对通信模板的组态。
- 实现了 SINEC-H1、SINEC-L2 及远程 I/O 系统三级子网的可靠互连
- 实现了操作管理站工控机（上位机）对现场控制站（下位机）中各点的数据采集。
- 为车间和工厂 CIMS 网的连接打下了良好的基础。

思考和展望

现场总线技术能在提高系统性能的同时降低系统成本。一项权威报告声称现场总线的应用将使控制系统的成本下降 67 %。巨大的经济利益正是世界各大工控公司积极参与竞争的原因。在现场总线市场处于“跑马圈地”阶段的关键时期，我国业界基本上是在犹豫中坐观其变，待国外发展初成气候后，我国在“九五”时方给予重视，重点进行了对基金会现场总线技术的研发，同时对其它主要总线也加以引进和消化吸收。最近有报道说我国通过对基金会现场总线协议的研究开发，已经掌握了现场总线的核心技术，跨入了世界先进行列。这的确令人鼓舞。但应当注意到，协议技术跨入世界先进行列远远不等于市场收益跨入世界先进行列。中国作为发展中国家，经济水平的不同决定了市场特点的不同，

现有的任何一种现场总线都难以做到对不同领域不同系统普遍适用。中国市场和第三世界市场尤其呼唤廉价可靠、灵活易用的中小系统现场总线。当前用户更急于呼唤现场总线对具体系统需求的适用性、匹配性和成本比较的评价体系。

有人断言，工控领域的 21 世纪是现场总线的世纪。发展和推广现场总线对于国民经济意义重大。现场总线技术的发展和推广应用有赖于其支撑体系的全面协调发展。其一，协议是现场总线技术的核心。简洁易用的协议是降低系统成本和提高用户亲和力的重要条件也是发展其它支撑技术的依据。其二，线缆。目前线缆不统一，不少公司采用自己的专用线缆，这恐怕是现场总线技术尚未成熟的明显特征。专用线缆的应用造成线缆的一次成本和维护成本都很高，系统维修改造时还要找原公司专门进口线缆，这对用户显然是不利的。我国应有针对性地发展几种流行现场总线的专用线缆，以配合现场总线的迅速发展。其三，圆卡。圆卡是协议的硬件接口，大幅度降低圆卡价格，是在我国迅速推广现场总线的重要条件。其四，组态系统。好的组态系统是现场总线综合性能的重要保证。研究高质量低价位的现场总线组态系统对于市场竞争非常重要。其五，现场总线人才。目前我国现场总线技术人才极为缺乏，需要大力加强培养，以适应未来自动测控系统普遍应用现场总线技术的需要。

致　谢

随着论文的完成，我将走向新的学习、生活和工作环境。在此，我向在整个攻读硕士学位期间关心和帮助我的老师和同学致以深深的谢意！特别感谢我的导师**恽小华**教授，以及**叶海荣**教授和**周白华**老师。在这两年半的研究生生涯中，他们不仅在学习上对我谆谆教导，而且在生活上给我细心的关怀和帮助，使我受惠终身。

另外，感谢通信教研室的各位老师和同学，感谢他们提供的优良环境和给我的启发。特别感谢南京邮电学院**金石**同学向我提供资料并对我的论文工作探讨启发。

最后，我要感谢我的父母以及我的亲人。多年来他们的勉励和支持给了我不断进取的动力。

主要参考文献

1　盐城八菱化纤 CIMS 系统总体设计报告．内部资料．1996

2　邱公伟.可编程控制器网络通信及应用.第2版.北京:清华大学出版社.2000

3　阳宪惠，徐庆燃．现场总线技术及其应用．第 3 版．北京：清华大学出版社．2001

4　Gerald Schickhuber, Oliver McCarthy. Distributed fieldbus and control network systems. Computing & Control Engineering Journal. 1997.8

5　阳宪惠，徐庆燃．互联网技术对现场总线技术发展的影响．自动化博览．2001(10.8)：71—75

6　王锦标，方崇智．过程计算机控制．第1版．北京：清华大学出版社．1992

7　姚远，刘国良．工业局域网SINEC L2的特点与应用．计算机自动测量与控制．1997(2)

8　王华强．工控组态软件的功能分析和应用实例．电气自动化．1998(4)

9　朱正伟．工控机中控制算法组态软件设计．自动化仪表．1998(5)

10　宁华，王志新．可编程序控制器网络通信技术及其应用研究．测控技术．1999(2)

11　郑宗汉．一个分散型控制系统中通信协议的实现．计算机应用．1999(5)

12　Jonas Berge. Fieldbus Enables Innovative Measurements. Advances in Instrumentation and Control. 1996: Vol.51

13　SIEMENS Corporation. SIMATIC S5-135U/155U System Manual. Release 06. 1993

14　SIEMENS Corporation. SIMATIC S5 S5-135U CPU928B Programming Guide. Release 01. 1994

15　SIEMENS Corporation. SIMATIC S5 STEP 5 Version 6.6 Manual. Release 01. 1996

16 PROFIBUS International Support Center. PROFIBUS Technical Description. Germany. 1999

17 SIEMENS Corporation. SIMATIC S5 308 Expansion Unit Interface Module Manual. Edition 04. 1998

18 SIEMENS Corporation. SIMATIC S5 318 Central Controller Interface Module Manual. Edition 04. 1998

19 SIEMENS Corporation. SIMATIC S5 SINEC L2 Interface of the S5 Programmable Controller Manual. Edition 02. 1993

20 景林. 可编程序控制器网络在纤维板生产中应用研究. 福建林学院学报. 2000 (20)

21 朱汝辉，张念祖，顾战松. 微机系统与可编程控制器之间的通信. 电气自动化. 1994(6)

22 赵永才. 浅议工业控制技术的发展趋势. 计算机应用. 1998(10)

23 瞿坦. 数据通信及网络基础. 第3版. 武汉：华中理工大学出版社. 1996

24 胡道元. 信息网络系统集成技术. 第2版. 北京：清华大学出版社. 1996

25 阳宪惠. CIMS网络系统的组成. 化工自动化及仪表. 1998(25)

26 吴功宜. 计算机网络基础. 第1版. 天津：南开大学出版社. 1996