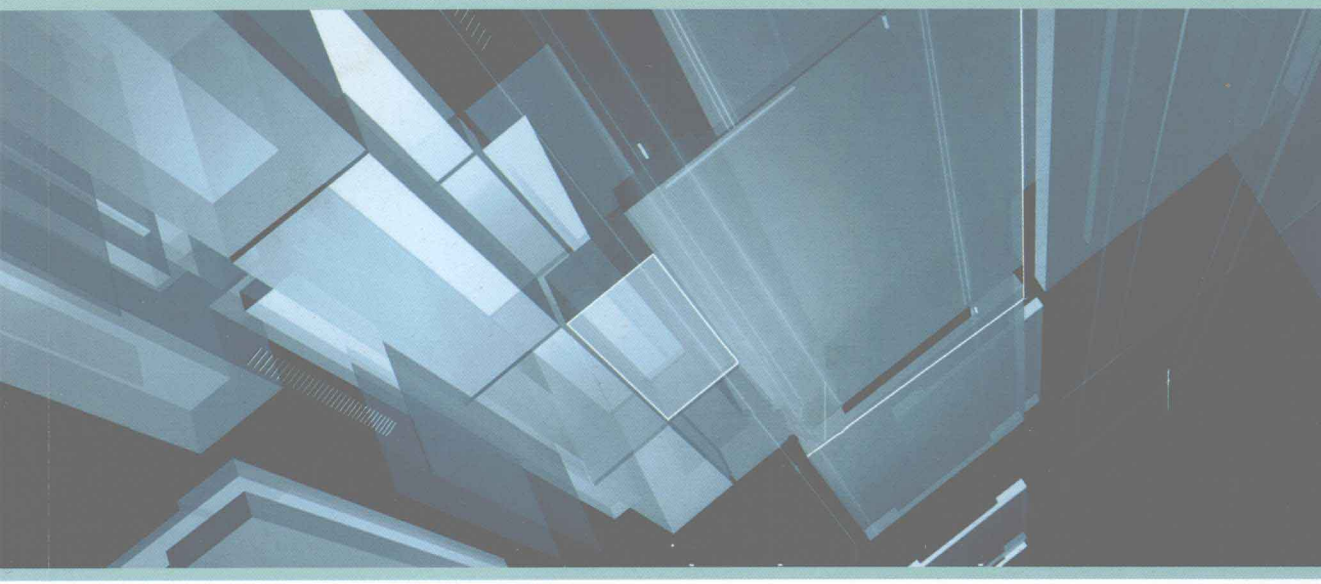
普通高等教育“十二五”规划教材



工业自动化网络

冯冬芹　王　酉　谢　磊　编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

普通高等教育“十二五”规划教材

工业自动化网络

编著　冯冬芹　王　酉　谢　磊
主审　仲崇权

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书为普通高等教育“十二五”规划教材。

本书除了第 1 章概述外，其他内容可以大体分为五部分。第一部分为网络基础知识部分，即第 2 章，介绍了通信技术基础。第二部分为计算机局域网部分，即第 3、4 章，介绍了计算机领域的常用局域网技术和标准。第三部分为传统现场总线部分，即第 5～9 章，重点介绍了工业应用领域比较典型且技术特点鲜明的现场总线技术，如 HART、MODBUS、CAN、FF、PROFIBUS 等。第四部分为工业以太网部分，即第 10 章，在介绍了工业以太网、实时以太网概念的基础上，重点介绍了 EPA、Ethernet/IP、EtherCAT 等工业实时以太网技术。第五部分为工业无线局域网部分，即第 11 章，主要包含了无线局域通信技术、蓝牙技术、Zigbee 通信技术、WiFi 通信技术、ISA100、无线 HART 协议、EPA 无线通信技术等。上述五个部分，第一部分是全书的基础，第二、三、四部分是全书的主题，第五部分是全书的延伸。

本书可作为普通高等院校自动化类、仪器仪表类、计算机类等相关专业的研究生和本科生教材，也可供从事网络控制工程工作的技术人员参考。

图书在版编目（CIP）数据

工业自动化网络 / 冯冬芹，王酉，谢磊编著. —北京：中国电力出版社，2011.7

普通高等教育“十二五”规划教材

ISBN 978-7-5123-1992-9

Ⅰ. ①工… Ⅱ. ①冯… ②王… ③谢… Ⅲ. ①工业企业－以太网－高等学校－教材 Ⅳ. ①TP393.18

中国版本图书馆 CIP 数据核字（2011）第 157003 号

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）

汇鑫印务有限公司印刷

各地新华书店经售

*

2011 年 9 月第一版 2011 年 9 月北京第一次印刷

787 毫米×1092 毫米 16 开本 17.125 印张 417 千字

定价 **30.00** 元

前　言

随着信息技术的迅速发展，现代工业生产正朝着规模化、自动化和信息化方向发展，人们对生产过程的安全、高效、优质、低耗、环保的要求不断提高，以追求更大的经济效益，从而推动了工业自动化网络的产生与发展。

自20世纪80年代中期开始，以现场总线、工业以太网、工业无线网络技术为代表的工业自动化网络对工业自动化仪表、控制系统的发展起着越来越重要的作用，并引导着工业控制系统朝着数字化、网络化、智能化、开放与集成化方向发展。

为了使自动化类、仪器仪表类、计算机类等专业的研究生和本科生、工程技术人员、科研工作者对现场总线技术有比较全面的了解，很多老师（如阳宪惠老师、甘永梅老师、刘泽祥老师、郑文波老师等）倾注了很多心血进行了研究，并出版了一些比较有影响的著作，成为很多大专院校的教材或教学参考书。

作者通过多年的现场总线本科生教学实践以及与其他部分院校老师的交流发现，由于条件限制，目前国内大多数院校尚未配备足够的现场总线实验装置与实验手段，这很容易使得学生对现场总线的理解局限在概念阶段，无法对其进行深入的理解和掌握。

基于此，作者结合近十年来的科研开发、标准制定与本科生教学经验，参考目前市场上已出版的相关书目、科研成果以及最新修订的国际标准，选取了目前在工业控制领域应用比较广泛、具有典型特点的局域网、现场总线、工业以太网、工业无线通信技术，从技术特点和工作原理的角度，进行解析、归纳与整理，并对一些细节性、比较抽象以及共有的技术进行了简化、概括，试图使这些技术易于读者的理解和掌握，也希望为读者今后可能进行的研究与学习提供一些参考和启示。

本书由浙江大学智能系统与控制研究所组织编写，其中，第1、2、3、10、11章由冯冬芹负责编写，第4、5、6、7章由王酉负责编写，第8、9章由谢磊负责编写。在教材编写过程中，得到了研究所所长褚健教授的关心与支持，同时作者的研究生来晓、张赫男、高汉荣、鲁立、贾凯丽、赵飞翔、陈鹏、田民杰等参与了部分章节的资料搜集与整理。本书由大连理工大学仲崇权教授主审，提出了宝贵的修改意见。在此一并向他们表示衷心的感谢。

本教材是基于大量的参考文献编写而成的，为此，对本书所参考的所有文献的作者表示诚挚的谢意。

由于时间仓促及作者知识的局限，加之当今自动化网络发展迅速，书中难免有不足或疏漏，敬请读者批评指正。

作者　于求是园

2011年6月

目　录

第1章 概 述

随着微电子技术、计算机技术、通信技术以及自动控制技术的不断发展，工业控制系统也朝着数字化、智能化、网络化与集成化方向不断发生着变革性的发展。本章将对工业控制系统、工业控制网络进行简单的回顾。

1.1 工业控制系统与控制网络

所谓工业控制网络，通俗地讲，是指应用于工业控制系统的网络通信技术，它是随着工业控制系统的发展而产生与发展起来的，是计算机网络技术、通信技术与控制技术相结合的产物。

众所周知，控制室和现场仪表之间的信号传输经历了以 4～20mA 为代表的模拟信号传输、以内部数字信号和 RS-232、RS-485 为代表的数字通信传输、以控制网络（包括现场总线、工业以太网、工业无线网络）为代表的网络传输三个阶段，这其中的每个阶段都伴随着工业控制系统的一次变革。特别是 20 世纪 80 年代产生的现场总线和互联网技术，对自动化控制系统带来了深刻的影响，使控制系统的信息交换除了传统的测量、控制数据外，更是扩展到了设备管理、档案管理、故障诊断、生产管理等管理数据领域，覆盖从工厂的现场设备层到控制、管理的各个层次，从工段、车间、工厂、企业到世界各地的市场，逐步形成了以工业控制网络为基础的企业综合自动化系统。

以现场总线和工业以太网为代表的工业控制网络已成为企业综合自动化体系的核心技术和核心部件，贯穿了整个企业综合自动化系统，如图 1-1 所示。

从企业综合自动化控制系统的角度看，工业控制网络从底向上依次为现场设备网、过程控制网、管理信息网等几个层次。

（1）现场设备网。对于分散控制系统（DCS）、可编程控制器（PLC）等传统控制设备而言，现场设备网就是系统控制器与现场输入输出设备或者卡件之间信息交换的通道，因此现场设备网又称作现场总线。现场设备是以网络节点的形式挂接在网络上，以实现控制器与现场设备、现场设备与现场设备之间的数据传输。因此，要求现场设备网必须具有可靠性高、时延确定性好、容错性好、安全性高等特点。

为满足这些特性，现场总线对 ISO/OSI 模型进行了简化，只采用其中的物理层、数据链路层和应用层，有的现场总线在应用层之上还增加了第 8 层（用户层），以实现特定用户信息的交换和传递。

（2）过程控制（监控）网。过程控制网又称作过程监控网，是用于连接控制室设备（如控制器、监视计算机、记录仪表等）的网络，连接在过程控制网上的设备从现场设备中获取数据，完成各种运算（特别是复杂控制运算）、运行参数的监测、报警和趋势分析、历史纪录、过程报表等功能，另外还包括控制组态的设计和安装。

过程控制网对数据传输的实时性要求不高，但对于网络带宽、可靠性、网络可用性的要

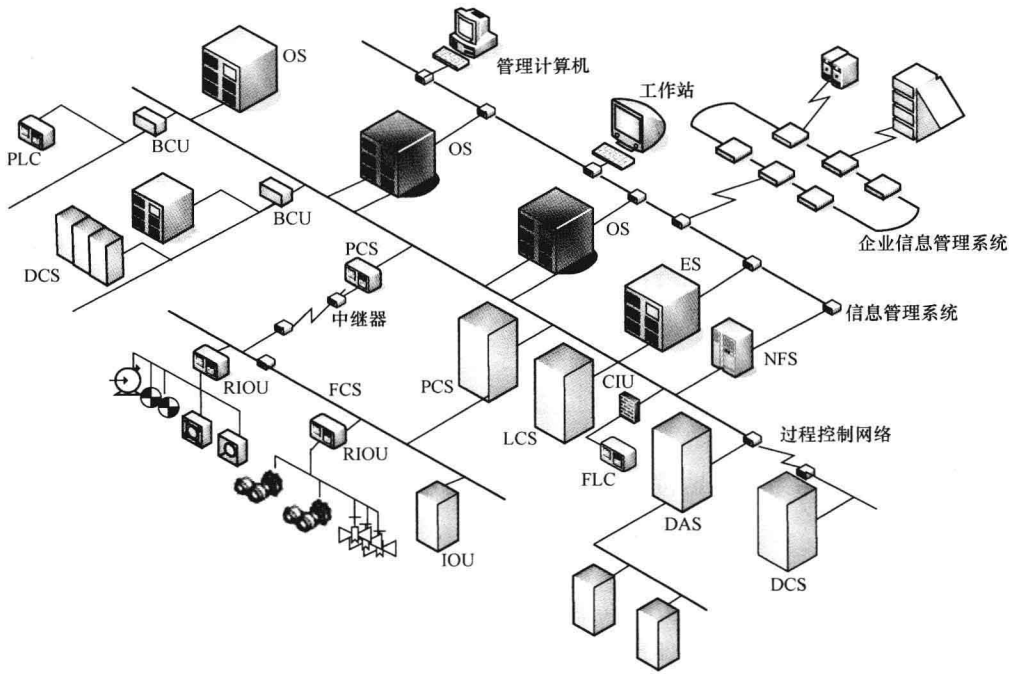


图 1-1 企业综合自动化系统网络架构图

OS—操作站；ES—工程师站；NFS—多功能计算站；BCU—总线变换单元；CIU—通信接口单元；FCS—现场总线控制系统；PCS—现场控制站；LCS—逻辑控制站；DAS—数据采集站；IOU—IO 单元；RIOU—远程 IO 单元

求是比较高的。20 世纪 80 年代，过程控制网一般采用 IEEE 802.4 的令牌网，而到了 90 年代末期，主流的控制系统（包括 DCS、PLC 等）一般都采用工业以太网。

（3）管理信息网。管理信息网的主要目的是在分布式网络环境下构建一个安全的网络系统。首先要将来自于过程控制网的信息转入管理层的关系数据库中，既可供企业管理层进行计划、排产、在线贸易等管理功能，又可供远程用户通过互联网了解控制系统的运行状态以及现场设备的工况，对生产过程进行实时的远程监控。

因此，管理信息网包括企业内部的局域网 Intranet 和互联网 Internet，由于涉及实际的生产过程，必须保证网络安全，可以采用的技术包括防火墙、用户身份认证以及密钥管理等。在这方面，工业以太网具有较大优势，兼容 TCP/IP，可以无缝连接 Internet，同时又不影响实时数据的传送，因此，整个控制网络可以采用统一的协议标准。

在整个工业通信网络模型中，现场设备层是整个网络模型的基础和核心，只有确保总线设备之间可靠、准确、完整的数据传输，上层网络才能获取信息以及实现监控功能。当前对现场总线的讨论多停留在底层的现场智能设备网段，但从完整的工业通信网络模型出发，在保证信息安全的前提下，应更多地考虑现场控制层与中间监控层、管理层，甚至与 Internet 层之间的数据传输与交互问题，以及实现控制网络与信息网络的紧密集成。

在以上几个层次的网络中，由于管理信息网一般采用的是互联网等公共网络资源，在本书中将不再详细介绍。因此，本书所指的工业控制网络仅包括现场设备网和过程控制网两个部分。

1.2 工业控制网络发展历程与特点

一、工业控制网络发展过程

工业控制网络的发展，经历了模拟信号传输、数字信号传输、现场总线、工业以太网，工业无线通信等几个阶段。

回顾工业控制系统的发展史可知，每一代新的控制系统的推出都是针对老一代控制系统存在的缺陷而给出的解决方案，同时也代表着技术的进步和效能的提高。

1. 模拟信号传输

20 世纪六七十年代模拟仪表控制系统占主导地位。其明显的缺点是模拟信号精度低、易受干扰。

2. 数字信号传输

20 世纪七八十年代集中式数字控制系统占主导地位。采用单片机、PLC 作为控制器使得在控制器内部传输的是数字信号，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。集中式数字控制系统的优点是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；不足的是，对控制器本身要求很高，必须具有足够的处理能力和极高的可靠性，当系统处理任务数量增加时控制器的效率和可靠性将急剧下降。

集散控制系统（DCS）是一种比较典型的运用数字传输技术的控制系统。DCS 自 20 世纪 70 年代产生以来，在市场上一直占据着主导地位。其核心思想是集中管理、分散控制，即管理与控制相分离，上位机用于集中监视管理功能，若干台下位机分散到现场，实现分布式控制，各上、下机之间通过控制网络互联实现相互之间的信息传递。这种分布式的控制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。在集散控制系统中，分布式控制思想的实现得益于网络技术的发展和应用。遗憾的是，不同的 DCS 厂家为达到垄断经营的目的而对其控制通信网络采用专用的封闭形式，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，集散控制系统从该角度而言实质上是一种封闭或专用的不具互操作性的分布式控制系统。而且 DCS 系统造价昂贵，综合上述情况，用户对网络控制系统提出了开放性、标准统一和降低成本的迫切要求。

3. 现场总线

现场总线控制系统（FCS）顺应控制系统开放性的要求，于 20 世纪 80 年代中期产生。与此同时，国际电工委员会（IEC）着手定义现场总线协议，用现场总线这一开放的、可互操作的网络将现场各控制器及仪表设备互连，同时控制功能彻底下放到现场，降低安装成本和维护费用。因此，FCS 实质上是一种开放的、具有可操作性的、彻底分散的分布式控制系统。但是由于各方利益的不同，现场总线没有能够形成统一的意见，导致多种总线林立，互相之间无法协调工作。在 1999 年，IEC 终于通过 IEC 61158 协议第二版，这是一个包括 8 种现场总线的协议集，更加确立了多种总线共存的局面。

4. 工业以太网

正是由于多总线并存，以太网在商用领域获得了巨大的成功，并且不断向工业领域延伸，

从2000年起，掀起了通过以太网统一现场总线的研究浪潮。以太网以其开放、高速、低成本、软硬件丰富等特点得以在工业领域广泛应用，技术标准的研究也越来越活跃，到2007年，包括中国制定的EPA在内的共11种工业以太网标准进入IEC标准体系。

5. 工业无线通信

在工业以太网获得极大发展的同时，现代数据通信系统发展的重要方向——无线局域网（Wireless LAN）技术也开始在工业控制网络中逐渐被应用。无线局域网技术可以非常便捷地以无线方式连接网络设备，在一些禁止或限制使用电缆的工业现场，无线局域网获得了一展身手的机会。虽然在商业通信领域，已经有较为成熟的无线通信技术推向市场，但在工业控制领域，无线局域网技术还处于试用阶段，通信技术和通信标准还未统一，各大公司正在加紧开发相关技术，希望在未来的市场竞争中占得先机。目前的研究方向主要集中在安全性、移动漫游、网络管理以及与3G等其他移动通信系统之间的关系等问题上。

二、工业控制网络特点

在网络集成式控制系统中，网络是控制系统运行的动脉，是通信的枢纽。工业控制网络作为一种特殊的网络，直接面向生产过程控制，肩负着工业生产运行一线测量与控制信息传输的特殊任务，并产生或引发物质或能量的运动和转换。

工业自动化网络作为一种特定应用的网络，和商业信息网络不同，具有自身的特点。

1. 系统响应的实时性

工业控制网络是与工业现场测量控制设备相连接的一类特殊通信网络，控制网络中数据传输的及时性与系统响应的实时性是控制系统最基本的要求。

工业控制系统的基本任务是实现测量控制，需要通过控制网络及时地传输现场过程信息和操作指令。控制系统中，有相当多的测控任务是有严格的时序和实时性要求的。若数据传输达不到实时性要求或因时间同步等问题影响了网络节点间的动作时序，就可能会造成灾难性的后果。因此不仅要求工业控制网络的传输速度快，而且还要求响应快，即响应实时性要好。

所谓实时性，是指控制系统能在较短并且可以预测确定的时间内，完成过程参数的采集、加工处理、控制运算、反馈执行等完整过程，并且执行时序满足过程控制对时间限制的要求。实时性表现在对内部和外部事件能及时地响应并做出相应的处理，不丢失信息、不延误操作。对于控制网络，处理的事件一般分为两类：一类是定时事件，如数据的定时采集、运算控制等；另一类是随机事件，如事故、报警等。对于定时事件，系统设置时钟，保证定时处理。对于随机事件，系统设置中断，并根据故障的轻重缓急预先分配中断级别，一旦事故发生，保证优先处理紧急故障。

控制网络通信中的媒体访问控制机制、通信模式、网络管理方式等都会影响到通信的实时性和有效性。

2. 开放性

这里的“开放”是指通信协议公开，不同厂商的设备可互连为系统，并实现信息交换；也指相关标准的一致性、公开性，强调对标准的共识与遵从。作为开放系统的控制网络，应该能与世界上任何地方的遵守相同标准的其他设备或系统连接。

遵循同一网络协议的测量控制设备应能够“互操作”与“互用”。“互操作”是指互连设备间可进行信息传送与沟通。“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，对于同一类型协议的不同制造商产品可以混合组态，构建成一个开放系统。

3. 极高的可靠性

工业控制网络必须连续运行，它的任何中断和故障都可能造成停产，甚至引起设备和人身事故，带来极大的经济损失。因此工业控制网络必须具有极高的可靠性，对于过程信息和操作指令等关键数据的传输，应实现“零”丢包率。

工业控制网络的高可靠性通常包含三个方面内容。

其一，可使用性好，网络自身不易发生故障。这要求网络设备质量高，平均故障间隔时间长，能尽量防止故障发生。提高网络传输质量的一个重要的技术是差错控制技术。

其二，容错能力强，网络系统局部单元出现故障，不影响整个系统的正常工作。如在现场设备或网络局部链路出现故障的情况下，能在很短的时间内重新建立新的网络链路。

在网络的可靠性设计中，主要强调的思想是尽量防止出现故障，但是无论采取多少措施，要保证网络 100%无故障是不可能的，也是不现实的。容错设计则是从全系统出发，以另一个角度考虑问题，其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，系统仍能完全正确地工作，也就是说给系统增加了容忍故障的能力。

提高网络容错能力的一个常用措施是在网络中增加适当的冗余单元，以保证当某个单元发生故障时能由冗余单元接替其工作，原单元恢复后再恢复出错前的状态。

其三，可维护性强，故障发生后能及时发现和及时处理，通过维修使网络及时恢复。这是考虑当网络系统万一出现失效时，系统能够采取安全性措施，如及时报警、输出锁定、工作模式切换等，同时具备极强的自诊断和故障定位能力，且能迅速排除故障。

4. 良好的恶劣环境适应能力

控制网络还应具有对现场恶劣环境的适应性。在这一点上，控制网络明显区别于办公室环境的各种网络。控制网络工作环境往往比较恶劣温度与湿度变化范围大，空气污浊、粉尘污染大，振动、电磁干扰大，并常常伴随有腐蚀性、有毒气体等。因此，要求工业控制网络必须具有机械环境适应性、气候环境适应性、电磁环境适应性或电磁兼容性（EMC），并满足耐腐蚀、防尘、防水等要求。不同工作环境对控制网络的环境适应性有不同的要求，工业控制网络设备需要经过严格的设计和测试，例如能在高温、严寒、粉尘环境下保持正常工作，能抗振动、抗电磁干扰，在易燃易爆环境下能保证本质安全，有能力支持总线供电等。

5. 安全性

工业自动化网络的安全性包括生产安全和信息安全两方面。在工业过程控制中，当涉及到容易燃烧和爆炸的原料时，因容器破损或泄漏，空气中含有挥发的爆炸性气体、粉尘等，这些区域称为危险区域。例如，石油及其衍生物、氢气、瓦斯、面粉等物质，一旦条件合适，都会引起爆炸。这就需要工业自动化网络中的控制设备具有本质安全的性能，利用安全栅技术，将提供给现场仪表的电能量限制在既不能产生足以引爆的火花，也不能产生足以引爆的仪表表面温升的安全范围内。

信息安全也是工业控制网络中非常重要的一个方面。在各种大中型企业的生产及管理控制过程中，哪怕是一点信息的失密或者遭到病毒破坏都有可能导致巨大的经济损失。因此，信息本身的保密性、完整性以及信息来源和去向的可靠性是整个工业控制网络系统必不可少的重要组成部分。在信息安全方面，网关是整个系统的有效屏障，它可以对经过它的数据包进行过滤。同时，随着加密解密技术与网络技术的进一步融合，工业自动化网络的信息安全

性也得到了进一步的保障。

1.3 常见工业控制网络

一、现场总线

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。现场总线原本是指现场设备之间公用的信号传输线，后来又被定义为应用在生产现场，在控制设备之间实现双向串行多节点数字通信的技术。随着技术内容的不断发展和更新，现场总线已经成为工业控制网络的代名词。

在现场总线控制系统中，传统的测量控制仪表内置专用微处理器，具有了数字计算和数字通信能力，并成为能独立承担某些控制、通信任务的网络节点。现场总线把多个测量控制仪表、计算机等作为节点连接成网络系统，通过公开、规范的通信协议，在位于生产控制现场的多个微机化自控设备之间以及现场仪表与用作监控、管理的远程计算机之间，实现数据传输与信息共享。它给自动化领域带来的变化犹如计算机网络、互联网给单台计算机带来的变化，标志着一个自动化新时代的开端。

现场总线是综合运用微处理器技术、网络技术、通信技术和自动控制技术的产物。由于内置有微处理器，现场自控设备具有了数字计算和数字通信能力，一方面提高了信号的测量、控制和传输精度；另一方面也丰富了控制信息的内容，可实现异地远程自动控制，如操作远在数百千米之外的电气开关等。现场总线设备与传统自控设备相比，拓宽了信息内容，提供了传统仪表所不能提供的如阀门开关动作次数、故障诊断等信息，便于操作管理人员更好更深入地了解生产现场和自控设备的运行状态。

由于现场总线强调遵循公开统一的技术标准，因而有条件实现设备的互操作性和互换性。也就是说，用户可以把不同厂家、不同品牌的产品集成在同一个系统内，并可在同功能的产品之间进行相互替换，使用户具有了自控设备选择、集成的主动权。

与传统控制系统相比，现场总线控制系统（FCS）有如下优点。

（1）全数字化。将企业管理与生产自动化有机结合一直是工业界梦寐以求的理想，但只有在 FCS 出现以后这种理想才有可能高效、低成本地实现。在采用 FCS 的企业中，用于生产管理的局域网能够与用于自动控制的现场总线网络紧密衔接。此外，数字化信号固有的高精度、抗干扰特性也能提高控制系统的可靠性。

（2）可实现分布式测量与控制。在 FCS 中各现场设备有足够的自主性，它们彼此之间相互通信，完全可以把各种控制功能分散到各种设备中，而不再需要一个中央控制计算机，实现了真正的分布式控制。

（3）双向的数据传输。传统的 4～20mA 电流信号，一条线只能传递一路信号。现场总线设备则在一条线上既可以向上传递传感器信号，也可以向下传递控制信息。

（4）自诊断。现场总线仪表本身具有自诊断功能，而且这种诊断信息可以送到中央控制室，以便于维护，而这在只能传递一路信号的传统仪表中是做不到的。

（5）节省布线及控制室空间。传统的控制系统每个仪表都需要一条线连到中央控制室，在中央控制室装备一个大配线架。而在 FCS 系统中多台现场设备可串行连接在一条总线上，这样只需较少的线进入中央控制室，大量节省了布线费用，同时也降低了中央控制室

的造价。

（6）仪表功能的多重化。数字、双向传输方式使得现场总线仪表可以摆脱传统仪表功能单一的制约，可以在一个仪表中集成多种功能，做成多变量变送器，甚至集检测、运算、控制于一体的变送控制器。

（7）开放性。现场总线不再是专有的协议，而是通过国际标准（如 IEC 61158）、地区标准、国家标准、行业标准发布的公开、开放的协议。

（8）互操作性。来自不同厂家、遵循同一协议的现场总线设备可以互操作，这样就可以在一个企业中由用户根据产品的性能、价格选用不同厂商的产品，集成在一起，避免了传统控制系统中必须选用同一厂家产品的限制，促进了有效的竞争，降低了控制系统的成本。

（9）智能化与自治性。现场总线设备能处理各种参数、运行状态信息及故障信息，具有很高的智能化，甚至在部件出现网络故障的情况下也能独立工作，大大提高了整个控制系统的可靠性。

正因为如此，现场总线技术自 20 世纪 90 年代初开始发展以来，一直是世界各国关注和发展的热点，目前具有一定规模的现场总线已有数十种之多，为了开发应用以及争夺市场的需要，世界各国所采用的技术路线基本上都在开发研究的过程中同步制定了各自的国家标准（或协会标准），同时力求将自己的协议标准转化成各区域标准化组织的标准。国际电工委员会（IEC）、国际标准化组织（ISO）、各大公司及世界各国的标准化组织对于现场总线的标准化工作都给予了极大的关注。现场总线技术在历经了群雄并起、分散割据的初始阶段后，尽管已有一定范围的磋商合并，但由于行业与地域发展等历史原因，加上各公司和企业集团受自身利益的驱使，致使现场总线的国际化标准工作进展曲曲折折。经历了十多年的纷争，1999 年形成了一个由 8 个类型组成的 IEC 61158 现场总线国际标准。该标准于 2003 年启动修订，于 2007 年底发布的第 2 版本，更是包括了 16 大类，成为国际上制定时间最长、意见分歧最大的国标之一。

二、工业以太网

现场总线的出现适应了工业控制系统向分散化、网络化和智能化发展的方向，并且促使目前的自动化仪表、DCS 和可编程控制器（PLC）等产品的体系结构和功能结构产生重大变革，导致工业自动化领域的一次更新换代。但是现场总线技术在其发展过程中也存在许多不足：

（1）现有的现场总线标准过多，仅国际标准 IEC 61158 就包含了 8 个类型，未能统一到单一标准上来；

（2）不同总线之间不能兼容，不能真正实现信息透明互访，无法实现信息的无缝集成；

（3）由于现场总线是专用实时通信网络，成本较高；

（4）现场总线的速度较低，支持的应用有限，不便于和 Internet 信息集成。

另外，以以太网（Ethernet）为代表的 COTS（Commercial Off-the-Shelf）通信技术却发展得非常迅速，得到全球的技术和产品支持。因为成本低、稳定性好和可靠性高、应用广泛、共享资源丰富等优点，Ethernet 已经成为最受欢迎的通信网络之一，它不仅垄断了办公自动化领域的网络通信，而且在工业控制领域管理层和控制层等中上层的网络通信中也得到了广泛应用，并有直接向下延伸应用于工业现场设备间通信的趋势。

从技术方面来看，与现场总线相比，以太网具有以下优势。

（1）应用广泛。以太网是目前应用最为广泛的计算机网络技术，受到广泛的技术支持。几乎所有的编程语言都支持 Ethernet 的应用开发，如 Java、Visual C++、Visual Basic 等。这些编程语言由于广泛使用，并受到软件开发商的高度重视，具有很好的发展前景。因此，如果采用以太网作为现场总线，可以保证多种开发工具、开发环境供选择。

（2）成本低廉。由于以太网的应用最为广泛，因此受到硬件开发与生产厂商的高度重视与广泛支持，有多种硬件产品供用户选择。而且由于其应用广泛，硬件价格也相对低廉。目前，以太网网卡的价格只有 PROFIBUS、FF 等现场总线的 1/10，而且随着集成电路技术的发展，其价格还会进一步下降。

（3）通信速率高。目前以太网的通信速率为 10Mbit/s、100Mbit/s，1000Mbit/s 以太网技术逐渐成熟并开始广泛应用，10Gbit/s 以太网正在研究中。以太网的通信速率比目前的现场总线快得多，可以满足对带宽有更高要求的需要。

（4）控制算法简单。优先权控制是比较复杂的。以太网没有优先权控制意味着访问控制算法可以很简单。它不需要管理网络上当前的优先权访问级（而令牌环和令牌总线系统都存在这个问题）。还有一个好处是，没有优先权的网络访问是公平的，任何站点访问网络的可能性都与其他站相同，没有哪个站可以阻碍其他站的工作。

（5）软硬件资源丰富。由于以太网已应用多年，人们对以太网的设计、应用等方面有很多的经验，对其技术也十分熟悉。大量的软件资源和设计经验可以显著降低系统的开发和培训费用，从而可以显著降低系统的整体成本，大大加快系统的开发和推广速度。

（6）不需要中央控制站。我们知道，令牌环网采用了“动态监控”的思想，需要有一个站负责管理网络的各种“家务”。传统令牌环网如果没有动态监测是无法运行的，但是以太网就不需要中央控制站，不需要动态监测。

（7）可持续发展潜力大。由于以太网的广泛应用，使它的发展一直受到广泛的重视和大量的技术投入。并且，在这个信息瞬息万变的时代，企业的生存与发展将很大程度上依赖于一个快速而有效的通信管理网络，信息技术与通信技术的发展将更加迅速，也更加成熟，由此保证了以太网技术不断地持续向前发展。

（8）易于与 Internet 连接。以太网能实现办公自动化网络与工业控制网络的信息无缝集成。因此，工业控制网络采用以太网，就可以避免其发展游离于计算机网络技术的发展主流之外，从而使工业控制网络与信息网络技术互相促进、共同发展，并保证技术上的可持续发展，在技术升级方面无需单独的研究投入。

随着通信实时性和确定性问题的解决，工业以太网已成功进入现场设备层，成为现场总线标准体系中最具生命力的成员，并成为现场总线主要的发展方向。

实时以太网技术是最近两年来迅速发展起来的新型现场总线技术，这些实时以太网技术与 EPA 一起，均将成为 IEC 61158 新的现场总线类型，并均作为实时以太网应用行规国际标准 IEC 61784-2 的子集。

国际电工委员会（IEC）于 2003 年 5 月成立的 SC65C/WG11（实时以太网工作组），制定了 IEC 61784-2“基于 ISO/IEC 8802.3 的实时应用系统中工业通信网络行规”国际标准，该标准吸收了包括浙江大学、中控集团等联合制定的 EPA（Ethernet for Plant Automation）在内的 10 种实时以太网技术，使 IEC 61158 中包含的现场总线（包括传统现场总线和实时以太网）

类型由原来的11种扩展到了20种（包括10种实时以太网技术）。其他的工业实时以太网协议有德国Siemens公司的PROFInet IO、美国Rockwell公司的Ethernet/IP、德国Beckhoff公司的EtherCAT、德国赫优讯（Hilscher）自动化系统有限公司的SERCOS-III、奥地利B&R公司的PowerLink、日本横河公司的Vnet、日本东芝公司的TCnet、法国施耐德公司的Modbus RTPS、丹麦的P-NET TCP等（见表1-1所示）。

表1-1 **现场总线协议类型**

类 型	技 术 名 称	类 型	技 术 名 称
Type1	TS61158现场总线	Type11	TCnet实时以太网
Type2	CIP现场总线	Type12	EtherCAT实时以太网
Type3	PROFIBUS现场总线	Type13	Ethernet Power Link实时以太网
Type4	P-NET现场总线	Type14	EPA实时以太网
Type5	FF-HSE高速以太网	Type15	Modbus-RTPS实时以太网
Type6	SwiftNet（被撤销）	Type16	SERCOS-Ⅰ、Ⅱ现场总线
Type7	WorldFIP现场总线	Type17	Vnet/IP实时以太网
Type8	INTERBUS现场总线	Type18	CC-Link现场总线
Type9	FFH1现场总线	Type19	SERCOS-III实时以太网
Type10	PROFINet实时以太网	Type20	HART现场总线

三、工业无线通信

工业无线通信技术是最近几年迅速发展起来的新型控制网络技术。无线通信的诸多优势推动了无线通信技术在工业自动化领域的应用。无线通信技术超越地域和空间的限制，在某些远程化、移动对象等应用场合中以绝对的优势取代有线网络。特别是在某些复杂的工业应用场合，不宜或者无法架设有线网络，无线网络将依靠其无法比拟的灵活性、可移动性和极强的可扩容性给出理想的解决方案。

一般来讲，应用于工业控制网络的无线通信技术，可分为远程无线通信技术和短程无线通信技术，其中远程无线通信技术包括无线电台远传技术、GSM远传技术、GPRS（CDMA）远传技术、3G远传技术等，而短程无线通信技术包括IEEE 802.11、IEEE 802.15、IEEE 802.15.4等。其中，基于IEEE 802.15.4的短程无线通信技术受到了自动化领域的广泛关注，特别是由美国仪器仪表、系统与自动化协会（ISA）制定的ISA-100和美国HART基金会制定的WirelessHART最具代表性和竞争性。

在国家“863”计划的支持下，我国中国科学院沈阳自动化研究所、浙江大学、机械工业仪器仪表综合技术经济研究所、重庆邮电大学、上海自动化仪表所、北京科技大学、西南大学、中科博微公司、浙江中控集团、东北大学、大连理工大学等十余家单位成立了“测量、控制用无线通信技术”国家标准起草工作组，所起草的WIA-PA也得到了国际电工委员会的承认和接受，目前正在计划制定为国际标准。此外，由浙江大学、中控科技集团联合牵头的EPA标准工作组，也制定了WirelessEPA工业无线通信协议，实现了EPA有线与无线网络的无缝连接。

1.4 本书基本结构

本书除了绪论外，其他内容可以大体分为五个部分。

第一部分为网络基础知识部分，即第 2 章，介绍了通信技术基础，重点摘录了与现场总线和工业以太网相关的计算机网络、通信、开放系统互联参考模型等基本概念和基本术语。理解这部分知识，对于掌握本书下面章节提到的各种现场总线和实时以太网可以起到积极作用。

第二部分为计算机局域网部分，即第 3、4 章，介绍了计算机领域的常用局域网技术和标准，包括 IEEE 802.3 标准与以太网、IEEE 802.5 标准与令牌环网、IEEE 802.4 标准与 ARCnet 令牌网以及 TCP/IP 协议，并对这三个主要的局域网进行了技术比较。

第三部分为传统现场总线部分，即第 5、6、7、8、9 章，重点介绍了工业应用领域主要的现场总线技术，如 HART、MODBUS、CAN、FF、PROFIBUS 等。之所以选择这几种现场总线，是因为它们具有较高的市场占有率，更重要的是它们均具有比较明显的技术特点。本教材重点是针对这些现场总线，介绍其技术特点、通信模型以及工作机理。

第四部分为工业以太网部分，即第 10 章，在介绍了工业以太网、实时以太网概念的基础上，重点介绍了 EPA、Ethernet/IP、EtherCAT 等在技术上具有代表性的工业实时以太网技术。希望读者能根据现场总线与工业以太网各自的优缺点进行比较。

第五部分为工业无线通信部分，即第 11 章。无线通信网络作为一个新兴的产业正在不断的发展，它主要包含了无线局域通信技术、蓝牙技术、Zigbee 通信技术、WiFi 通信技术，ISA100、无线 HART 协议、EPA 无线通信技术等几个方面。了解这些无线通信知识，可以帮助我们更好地理解无线通信网络；在具体实践中，还应该根据实际情况，实际分析。

上述五个部分，第一部分是全书的基础，第二、三、四部分是全书的主题，第五部分是全书的延伸。通过对本书基本结构的说明，希望给读者一定的启示。