王 平 谢昊飞 肖 琼 向 敏 陈敏娜 著

工业以太网技术

科学出版社
www.sciencep.com

工业以太网技术

王 平 谢昊飞 肖 琼 向 敏 陈敏娜 著

科学出版社
北京

内 容 简 介

网络技术的迅速发展引发了自动控制领域的深刻技术变革，以现场总线和工业以太网技术为代表的控制网络技术是现代自动控制技术与信息网络技术相结合的产物，是下一代自动化设备的标志性技术，是改造传统工业的有力工具，也是信息化带动工业化的重点方向。目前网络控制技术正从传统的控制网络技术——现场总线向现代控制网络技术——工业以太网技术的方向发展。

本书系统地介绍了工业以太网的技术原理、设计方法与产品开发技术。结合开发 EPA 控制网络的大量典型例子，重点介绍了 EPA 协议栈软件、确定性通信调度方法、EPA 协议实现技术、高功率以太网总线供电技术与设备、面向测量与控制的精确时间同步方法、基于 XML 的 EPA 设备描述与功能块解析、EPA 协议可执行测试集的形式化描述与一致性测试方法、EPA 网络安全技术等一系列关键技术问题的解决方案与实现技术。

本书主要面向自动控制领域从事科学研究、产品开发与工程应用的科研人员、工程技术人员，也可作为自动化、计算机、通信、测控、电气等专业高年级本科生及研究生的参考用书。

图书在版编目(CIP)数据

工业以太网技术/王平等著. —北京：科学出版社，2007

ISBN 978-7-03-019242-4

Ⅰ.工… Ⅱ.王… Ⅲ.工业控制-以太网 Ⅳ.TP393.11

中国版本图书馆 CIP 数据核字(2007)第 092668 号

责任编辑：余 丁 / 责任校对：宋玲玲
责任印制：刘士平 / 封面设计：嘉华永盛

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2007 年 7 月第 一 版 开本：B5(720×1000)
2007 年 7 月第一次印刷 印张：22 3/4
印数：1—2 500 字数：445 000

定价：60.00 元

(如有印装质量问题，我社负责调换〈科印〉)

前　言

随着微电子技术的发展，微型计算机的应用迅速渗透到各个领域。控制领域中计算机应用从单片机、可编程控制器、微机系统到工业控制网络，推动了生产方式的革命。计算机控制技术成为工业控制中最有潜力、最活跃的一个领域。目前，及时、准确、可靠地获得现场设备的信息是计算机控制系统的基本要求，可靠、高效的现场控制网络则是迅速有效地收集和传送现场生产与管理数据的基本保障。目前，网络技术的迅速发展引发了自动控制领域的技术变革。计算机控制系统的结构沿着网络化方向，控制系统体系结构沿着开放性方向发展将是计算机控制技术发展的大潮流，网络化、开放化、智能化和集成化是工业控制技术发展的方向与灵魂。现场总线技术、工业以太网技术、分布式网络控制技术与企业网络技术的出现及其发展，将推动控制领域的全方位技术进步。

本书作者作为核心成员参与制定的新一代现场总线标准——《用于工业测量与控制系统的 EPA 通信标准》成为我国第一个拥有自主知识产权并被 IEC 认可的工业自动化领域国际标准（IEC/PAS62409），并作为实时以太网国际标准 IEC 61748-2 与现场总线国际标准 IEC61158（修订版）的第 14 个子集进行制定。重庆邮电大学与浙江大学、浙江浙大中控技术有限公司、中国科学院沈阳自动化所等单位解决了 EPA（Ethernet for Plant Automation）协议栈软件、基于 XML 的 EPA 设备描述与功能块解析、确定性通信调度方法、EPA 协议实现技术、高功率以太网总线供电技术与设备、面向测量与控制的精确时间同步方法、EPA 协议可执行测试集的形式化描述与一致性测试方法、EPA 网络安全技术、基于 OPC 的系统集成技术等一系列关键技术问题，形成了具有自主知识产权的 EPA 核心技术，实现了原创性技术创新。改变了我国现场总线长期所处的跟踪研究、核心技术始终掌握在国外跨国企业手中的被动局面，使我国在新一轮的实时以太网技术发展中处于平等竞争的状态。本书以计算机控制系统的网络化、开放化、智能化和集成化发展趋势为主线索，有机地融入了作者多年参加国家 863 项目与国家/国际标准起草的科研成果，以作者所在课题组解决的 EPA 系列关键技术问题与具有自主知识产权的 EPA 核心技术为基础，系统地介绍了工业以太网的技术原理、设计方法与产品开发技术。

本书编写过程中力求做到理论分析与技术应用并重，注重系统性、实用性，强调工业控制网络理论与技术的实际运用。为了便于读者理解和掌握，列举了大量有关 EPA 网络产品与 EPA 现场仪表开发的典型例子，并力求达到重点突出，

层次分明，语言精练，易于理解。

全书共分八章，第一章介绍了工业控制网络的发展历程与趋势；第二章介绍了工业控制网络的技术基础；第三章介绍了工业以太网技术标准体系，并对目前影响较大的工业以太网技术进行了分析；第四、五、六章分别介绍了作者在EPA控制网络的关键技术与解决方法、EPA的网络产品与开发方法、主要EPA现场仪表产品与开发技术等方面的研究成果；第七章介绍了作者开发的代表目前现场总线发展趋势的基于功能块的组态软件及其开发技术；第八章介绍了EPA协议测试方法与技术，包括一致性测试、互操作性测试与通信性能测试等方面的研究成果。

本书是重庆邮电大学控制网络技术研究所全体同仁多年来在工业控制网络、控制系统等方面从事研究、开发与应用工作的总结。本书由王平、谢昊飞、肖琼、向敏、陈敏娜著述，参与本书著述的人员还有孙攀、袁李、王浩、王浩文、楼正华、干开峰（第四章），金渝、袁李、孙攀、唐铬、杨震斌（第五章），金渝、孙攀、杨夏、付尉（第六章），张杰、梁云鹏、周菲、戴琼瑶（第七章），陈良华、汪春华、张艳芳（第八章）。同时本书在著述过程中还引用了国家863计划EPA项目组的研究成果，并得到了浙江大学冯冬芹、中科院沈阳自动化所王宏与徐皑冬、大连理工大学仲崇权、清华大学杨佃福、中国四联仪器仪表集团公司张军的关心与支持。在此对他们表示衷心的感谢。

作者

2007年3月于重庆邮电大学

目　　录

第一章　工业控制网络的发展

以现场总线与工业以太网技术为代表的控制网络技术是现代自动控制技术和信息网络技术相结合的产物，是下一代自动化设备的标志性技术，是改造传统工业的有力工具，也是信息化带动工业化的重点方向。目前网络控制技术正在从传统控制网络技术——现场总线向现代控制网络技术——工业以太网技术发展。

1.1　工业控制网络的特点

1.1.1　工业控制网络与信息网络的区别

工业控制网络作为一种特殊的网络，直接面向生产过程和控制，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。因此，它通常应满足强实时性与确定性、高可靠性与安全性、工业现场恶劣环境的适应性、总线供电与本质安全等特殊要求。较之信息网络，工业控制网络具有如下区别：

① 工业控制网络传输的信息多为短帧信息，长度较小，且信息交换频繁；而信息网络传输的信息长度大，互相交换的信息不频繁。

② 工业控制网络周期与非周期信息同时存在，正常工作状态下，周期性信息（如过程测量与控制信息、监控信息等）较多，而非周期信息（如突发事件报警、程序上下载等）较少；而信息网络非周期信息较多，周期信息较少。

③ 一般来说，过程控制网络的响应时间要求为 0.01～0.5s，制造自动化网络的响应时间要求为 0.5～1.0s；而信息网络响应时间要求为 2.2～6.0s，信息网络大部分应用的响应实时性可以忽略。

④ 工业控制网络的信息流向具有明显的方向性，如测量信息由变送器向控制器传送，控制信息由控制器向执行机构传送，过程监控与突发信息由现场仪表向操作站传送，程序下载由工程师站向现场仪表传输等；而信息网络的信息流向不具有明显的方向性。

⑤ 工业控制网络中测量控制信息的传送有一定的顺序性，如测量信息首先需要传送到控制器，由控制器进行控制运算，发出的控制信息传送给执行机构，控制相关执行机构的动作；而信息网络的信息传送没有一定的顺序性。

⑥ 工业控制网络应具有良好的环境适应性，即在高温、潮湿、振动、腐蚀、

电磁干扰等工业环境中具有长时间、连续、可靠、完整地传送数据的能力，并能抗工业电网的浪涌、跌落和尖峰干扰；而信息网络对环境适应性的要求不高。

⑦ 在可燃与易爆场合，工业控制网络还应具备本安防爆性能；而信息网络不需要本安防爆性能。

⑧ 工业控制网络的通信方式多为广播或组播的通信方式；而信息网络的通信方式多为点对点的通信方式。

⑨ 工业控制网络必须解决多家公司产品与系统在同一网络中的相互兼容问题，即协议一致性与互操作性问题；而信息网络只需要解决互联互通问题，即协议一致性问题。

1.1.2　工业控制网络的技术特征

1. 系统的开放性与分散性

控制网络的出现使控制系统的体系结构发生了根本性改变，形成了在功能上管理集中、控制分散，在结构上横向分散、纵向分级的体系结构。把基本控制功能下放到现场具有智能的芯片或功能块中，不同现场设备中的功能块可以构成完整的控制回路，使控制功能彻底分散，直接面对对象，把同时具有控制、测量与通信功能的功能块与功能块应用进程作为网络节点，采用开放的控制网络协议进行互联，形成底层控制网络。图 1-1 所示为集散控制系统（distributed control system，DCS）向现场总线控制系统（Fieldbus control system，FCS）的演变示意图。

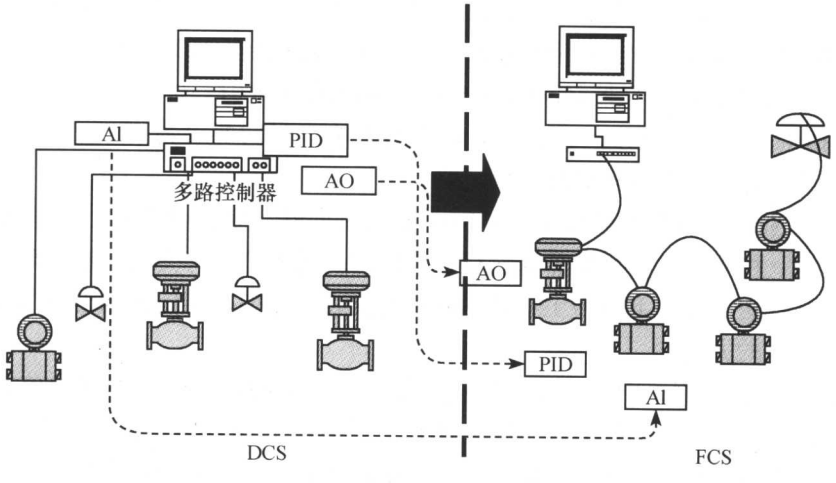

图 1-1　DCS 向 FCS 的演变

2. 系统响应的实时性与确定性

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。在工业自动化控制中需要及时地传输现场过程信息和操作指令，工业控制网络不但要完成非实时信息的通信，而且还要求支持实时信息的通信。这就不仅要求工业控制网络传输速度快，而且还要求响应快，即响应实时性要好。所谓实时性是在网络通信过程中能在线实时采集过程的参数，实时对系统信息进行加工处理，并迅速反馈给系统完成过程控制，满足过程控制对时间限制的要求。同时要求网络通信任务的行为在时间上可以预测确定。实时性表现在对内部和外部事件能及时地响应，并作出相应地处理，不丢失信息，不延误操作。工业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。

对于控制网络，它主要的通信量是过程信息及操作管理信息，信息量不大，传输速率一般不高于1Mb/s，信息传输任务相对比较简单，但其实时响应时间要求较高，为0.01～0.5s。除了控制管理计算机系统的外部设备外，还要控制管理控制系统的设备，并具有处理随机事件能力。实际操作系统应保证在异常情况下及时处置，保证完成任务，或完成最重要的任务，要求能及时发现并纠正随机性错误，至少保证不使错误影响扩大，应具有抵制错误操作和错误输入信息的能力。

3. 网络产品要具有互操作性与互用性

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，使它具有互操作性。一致性测试是通过一系列具体应用，对现场总线的硬件和软件产品进行的行为测试，以确定具体应用中的行为与相应的协议标准一致，从而确定被测设备或系统对通信协议的各种应用与现场总线标准规范的符合程度。互操作性是指在没有任何功能损失的条件下，不同厂家的多个设备可以在一个系统中协同工作，即这些设备能够实现控制功能上的相互连接与操作。因此，各制造商产品要通过所属各类总线协议符合其规定的一致性测试及互操作性测试，并通过专门的测试认证。

4. 要求极高的可靠性

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。因此工业控制网络必须具有极高的可靠性，如工业控制网络要求过程信息和操作指令实现零丢包率。

工业控制网络的高可靠性通常包含三个方面内容：

① 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。

② 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，主要强调的是尽量防止出现故障，但是无论采取多少措施，要保证网络绝对无故障是不可能的，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。

③ 可维护性高，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，系统一是要能采取安全性措施，如及时报警、输出锁定、工作模式切换等；二是要能具有极强的自诊断和故障定位能力，且能迅速排除故障。

5. 需要良好的恶劣环境适应能力

工业控制网络应具有良好的环境适应性，即工业控制网络强调恶劣环境下数据传输的完整性、可靠性。由于工业生产现场环境与一般商业环境不同，如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。由此，要求工业控制网络必须具有机械环境适应性（如耐振动、耐冲击）、气候环境适应性（工作温度要求为－40～85℃，至少为－20～70℃，并要耐腐蚀、防尘、防水）、电磁环境适应性或电磁兼容性 EMC 等要求，在这些指标上工业控制网络设备需要经过严格的设计和测试。

6. 必须具备严格的网络安全性

工业控制网络主要用于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，更不要说由于敌对者的恶意破坏而导致网络的不能正常运行了。因此，信息本身的保密性、完

整性、鉴别性以及信息来源和去向的可靠性是每一个管理者和操作者始终不可忽视的，也是整个工业控制网络系统必不可少的重要组成部分。

1.2　传统控制网络——现场总线的发展

1.2.1　现场总线的定义

现场总线是网络技术向工业生产现场发展的产物，是在市场需求的背景下发展起来的新型技术。具有全数字化、分散、双向传输和多分支的特点，其关键标志是能支持双向、多节点、总线式的全数字通信。现场总线技术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，它把专用微处理器引入传统的现场仪表，使它们各自都具备数字计算和数字通信能力，成为能独立承担某些控制、通信任务的网络节点。

现场总线的概念是随着微电子技术的发展，数字通信网络延伸到工业过程现场成为可能后，于1984年左右提出的。根据国际电工委员会IEC1158（后改为IEC61158）定义，现场总线是“安装在生产过程区域的现场设备、仪表与控制室内的自动控制装置、系统之间的一种串行、数字式、多点通信的数据总线”。或者说，现场总线是应用在生产现场、连接智能现场设备和自动化测量控制系统的数字式、双向传输、多分支结构的网络系统与控制系统，它以单个分散的、数字化、智能化的测量和控制设备作为网络节点，用总线相连接，实现相互交换信息，共同完成自动控制功能。其中，“生产过程”应包括断续生产过程和连续生产过程两类。现场设备、仪表指位于现场层的传感器、驱动器、执行机构等设备。因此，现场总线是面向工厂底层自动化及信息集成的数字化网络技术。

1.2.2　现场总线技术的发展历程

1983年，Honeywell推出了智能化仪表，它在原模拟仪表的基础上增加了具有计算功能的微处理器芯片，在输出的4～20mA直流信号上叠加了数字信号，使现场与控制室之间的连接模拟信号变为数字信号。之后，世界上各大公司推出了各种智能仪表。智能仪表的出现为现场总线的诞生奠定了基础。

1984年美国Inter公司提出一种计算机分布式控制系统位总线（Bitbus），它主要是将低速的面向过程的输入输出通道与高速的计算机多总线（Multibus）分离，形成了现场总线的最初概念。20世纪80年代中期，美国Rosemount公司开发了一种可寻址的远程传感器（HART）通信协议。采用在4～20mA模拟量叠加了一种频率信号，用双绞线实现数字信号传输。HART协议已是现场总线

的雏形。1985 年由 Honeywell 和 Bailey 等大公司发起，成立了 WorldFIP 并制定了 FIP 协议。1987 年，以 Siemens、Rosemount、横河等几家著名公司为首也成立了一个专门委员会并制定了 Profibus 协议。后来美国仪器仪表学会也制定了现场总线标准 IEC/ISA SP50。随着时间的推移，世界逐渐形成了两个针锋相对的互相竞争的现场总线集团：一个是以 Siemens、Rosemount、横河为首的 ISP 集团；另一个是由 Honeywell、Bailey 等公司牵头的 WorldFIP 集团。1994 年，两大集团宣布合并，融合成现场总线基金会（Fieldbus Foundation，FF）。对于现场总线的技术发展和标准制定，基金委员会取得以下共识：共同制定遵循 IEC/ISA SP50 协议标准；商定现场总线技术发展阶段时间表。

现场总线发展迅速，处于群雄并起、百家争鸣的阶段。围绕着现场总线技术的标准化，世界上各大厂商展开了激烈竞争，并主要形成了 FF 和 Profibus 两大阵营，都希望能够统一整个世界市场，但未能成功。经过 14 年的纷争，IEC 的现场总线标准化组织经投票，最后通过妥协出现了协调共存、共同发展的局面，以下这八种现场总线成为 IEC61158 现场总线标准，即：FF H1、ControlNet、Profibus、Interbus、P-Net、WorldFIP、SwiftNet、FF 之高速 Ethernet 即 HSE。其中，P-Net 和 SwiftNet 是专用总线；ControlNet、Profibus、WoldFIP 和 Interbus 是从 PLC 发展而来的；而 FF 和 HSE 是从传统 DCS 发展而来的。这八种现场总线采用的通信协议完全不同，因此，要实现这些总线的兼容和互操作是十分困难的。事实上，目前国际上有 40 多种现场总线，如 Interbus、Bitbus、DeviceNet、Modbus、Arcnet、P-Net、FIP、ISP 等，其中最具影响力的有五种，分别是 FF、Profibus、HART、CAN 和 LonWorks。这些现场总线还没有任何一种现场总线能覆盖所有的应用面，按其传输数据的大小可分为三类：传感器总线（Sensorbus）属于位传输；设备总线（Devicebus）属于字节传输；现场总线属于数据流传输。

由于技术出发点不同，目前的现场总线大都有各自的应用范围与应用领域。主要的现场总线的应用领域如图 1-2 所示。

① 过程控制：FF、Profibus-PA、HART、WorldFIP。

② 制造业自动化：Profibus-DP、Interbus。

③ 农业、养殖业、食品加工业：P-Net。

④ 楼宇自动化：LonWorks、Profibus-DP。

⑤ 汽车检测、控制：CAN。

⑥ 航空航天检测与控制：SwiftNet。

1.2.3 现场总线技术的发展趋势

现场总线技术的发展应体现为两个方面：一是低速现场总线领域的继续发展