



冯冬芹 褚健 金建祥 鲁立 著

实时工业以太网技术

——EPA及其应用解决方案

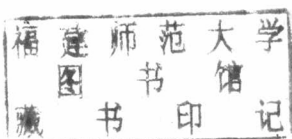


科学出版社

国家科学技术学术著作出版基金资助出版

实时工业以太网技术—— EPA 及其应用解决方案

冯冬芹 褚健 金建祥 鲁立 著



1041104



T1041104

科学出版社

北京

内 容 简 介

以太网以其价格低廉、应用广泛、传输速率高、可靠性高、易于组网等诸多优点,成为现今工业自动化领域应用最为广泛的数据通信技术。本书分析了以太网应用于工业自动化控制系统必须解决的重要关键技术问题,并针对这些问题,重点介绍我国第一个拥有自主知识产权的新一代工业以太网国际标准——EPA 在确定性与实时性通信机制、多网段系统设计、线缆与安装技术、网络可用性、功能安全、网络安全等方面的解决思路,并对 EPA 应用组态进行了介绍,期望使读者对 EPA 实时以太网应用方案以及技术特点有一个全面的认识和掌握。

本书可供自动化、仪器仪表等专业的研究生参考,还可作为现场总线通信技术相关的工程技术人员、科研工作者和学生参考书。

图书在版编目(CIP)数据

实时工业以太网技术: EPA 及其应用解决方案/冯冬芹等著. —北京:科学出版社, 2012

ISBN 978-7-03-035862-2

I. ①实… II. ①冯… III. ①工业企业-以太网 IV. ①TP393.18

中国版本图书馆 CIP 数据核字(2012)第 253237 号

责任编辑:张海娜 / 责任校对:林青梅

责任印制:张 倩 / 封面设计:耕者设计

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>

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2013 年 1 月第 一 版 开本: B5(720×1000)

2013 年 1 月第一次印刷 印张: 16 1/4

字数: 327 000

定价: 65.00 元

(如有印装质量问题,我社负责调换)

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、自动化和信息化的方向发展。20 世纪 80 年代中期产生的现场总线,将智能现场设备和自动化系统以全数字式、双向传输、多分支结构的通信控制网络连接,使工业控制系统向分散化、网络化和智能化发展成为可能,使工业控制系统的体系结构和功能结构产生重大变革。

以太网具有价格低廉、应用广泛、传输速率高、可靠性高、易于组网等诸多优点,而且拥有大量安装维护人员。它不仅垄断了信息领域的通信网络,而且成为工业应用领域的主流通信网络。

EPA 是 Ethernet for Plant Automation 的缩写,它基于以太网技术,针对工业自动化测量与控制系统的应用特点,进行了技术改造,适用于测量、控制等工业场合,并被国际电工委员会(International Electrotechnical Commission, IEC)发布为现场总线国际标准 IEC 61158/TYPE14,由此开创了我国实质性制定工业自动化国际标准的先河。

为了使自动化、仪器仪表等专业的学生、工程技术人员以及科研工作者对 EPA 实时以太网技术有比较全面的了解,作者基于近十年来对 EPA 工业实时以太网技术的科研开发、标准制定和实践经验,从技术特点和工作机理的角度,对 EPA 技术进行解析、归纳与整理,而对一些细节性、比较抽象以及共有的技术进行了简化、概括,试图使读者易于理解和掌握,也希望给读者的相关研究和应用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,集中了研究所和浙江中控科技集团有限公司的 EPA 研究团队十几来的智慧和研究成果,如专利、论文、教材、标准、技术文档等。在本书编写过程中,赵联祥、桂本煊、陈高翔、刘世龙、陈佳、章涵、杨大胜、来晓、赵飞翔、田明杰、朱杰、张淑兰、王强、唐建生、陈鹏、贾凯丽、陈建、马振芳、仇荔、朱予辰、傅东旭、李志强等项目组成员参与了部分章节关键技术成果的开发与资料搜集整理,在此对他们表示衷心的感谢!同时也要感谢在 EPA 标准化过程中长期良好合作的中国科学院沈阳自动化研究所的王宏、徐皑冬研究员,大连理工大学的仲崇权教授,重庆邮电大学的王平教授,以及清华大学的杨佃福教授等。

本书还引用了部分文献,对其作者表示诚挚的谢意。

由于作者水平有限,加之当今工业以太网技术发展迅速,书中难免存在不足之处,敬请读者批评指正并提出宝贵意见。

作者

2012 年 8 月于浙江大学求是园

目 录

前言

第 1 章 绪论	1
1.1 控制系统发展回顾	1
1.2 工业控制网络	4
1.3 工业以太网与实时以太网	8
1.4 EPA 技术与标准	13
参考文献	16
第 2 章 EPA 确定性与实时性通信技术	18
2.1 以太网的通信“不确定性”	18
2.2 EPA 确定性通信机制	20
2.2.1 EPA 确定性通信链路层模型	21
2.2.2 EPA 确定性通信调度模型	23
2.2.3 EPA 确定性通信调度规程	25
2.2.4 EPA 时钟同步	27
2.3 EPA-FRT 强实时通信技术	28
2.4 EPA-BRT 数据流业务实时通信技术	33
2.5 EPA 协议簇几种实时通信技术的比较	36
2.6 EPA 实时性能分析	38
2.7 基于 EPA 的通信调度规划	50
2.8 小结	53
参考文献	53
第 3 章 EPA 多网段设计技术	56
3.1 控制系统中的分网段技术	56
3.2 EPA 多网段结构	57
3.3 EPA 网桥	60
3.4 EPA 无线网段接入	67
3.4.1 无线局域网微网段及其接入	68
3.4.2 蓝牙微网段及其接入	70
3.5 二层式 EPA 微网段及其子网划分	71

3.6 EPA 多网段系统特点及性能分析	74
3.7 小结	77
参考文献	77
第4章 EPA 线缆与安装技术	79
4.1 总体要求	79
4.2 EPA 线缆与安装总体特性	81
4.2.1 网络拓扑的设计	81
4.2.2 通信介质	83
4.3 EPA 网络供电	84
4.4 EPA 本质安全与安全防护	88
4.5 接地系统、雷击浪涌与防护	95
4.5.1 接地/等电位连接/参考地	95
4.5.2 雷击浪涌与防护	97
4.6 小结	101
参考文献	101
第5章 EPA 网络可用性技术	102
5.1 工业以太网的可用性	102
5.2 分布式环网冗余技术	104
5.3 DRP 冗余故障自诊断与自恢复	106
5.4 DRP 与 EPA 协议的协同应用	113
5.5 DRP 性能评估	121
5.6 小结	128
参考文献	128
第6章 EPA 功能安全通信技术	130
6.1 功能安全与功能安全通信	130
6.1.1 安全功能响应时间	132
6.1.2 功能安全通信模型	132
6.1.3 工业控制网络通信的风险	134
6.2 EPA 功能安全通信方案	136
6.2.1 EPASafety 安全通信概念	136
6.2.2 EPASafety 协议结构	137
6.2.3 EPASafety 系统架构	137
6.2.4 EPA 功能安全通信流程	138

6.3	EPA 功能安全通信应对风险的解决措施	144
6.3.1	主要的 EPASafety 解决方法及与风险的对应关系	144
6.3.2	实例分析	146
6.4	EPA 功能安全通信 SIL 等级评估方法	148
6.4.1	EPASafety 通信模型 SIL 等级计算方法	148
6.4.2	EPASafety 通信模型的 SIL 等级计算结果	149
6.5	小结	149
	参考文献	149
第 7 章	EPA 网络安全技术	150
7.1	工业控制系统的安全问题	150
7.1.1	工业控制系统网络的定义和特点	150
7.1.2	工业控制系统网络安全的提出和意义	150
7.1.3	IT 系统与工业控制系统的差异	151
7.2	EPA 安全概述	154
7.2.1	EPA 网络安全特点	154
7.2.2	EPA 网络安全的脆弱性分析	154
7.2.3	EPA 安全威胁与安全目标	155
7.3	EPA 纵深防御网络安全技术	155
7.3.1	EPA 网络安全结构	156
7.3.2	EPA 系统安全域边界控制器	157
7.3.3	EPA 主机安全监控代理	158
7.3.4	EPA 工业安全交换机	158
7.3.5	EPA 监控层防火墙	159
7.3.6	EPA 安全网桥	160
7.3.7	EPA 系统统一智能安全管理平台	161
7.4	小结	164
	参考文献	165
第 8 章	EPA 功能块应用进程与设备描述	166
8.1	EPA 功能块	166
8.1.1	EPA 功能块与互可操作	166
8.1.2	EPA 功能块的定义	167
8.1.3	EPA 基本功能块、复合功能块	172
8.2	功能块的链接与通信	179

8.2.1 EPA 功能块应用进程	179
8.2.2 功能块与链接对象	180
8.2.3 功能块与通信栈的通信	182
8.2.4 功能块的组态	183
8.3 设备描述	184
8.3.1 设备描述格式	185
8.3.2 设备描述要素	188
8.3.3 设备描述文件的解析	189
8.4 设备描述功能块应用举例	190
8.4.1 设备模型	190
8.4.2 EPA 功能块模型	193
8.4.3 应用举例	194
8.5 小结	197
参考文献	198
第9章 EPA 测试技术	199
9.1 EPA 测试的内容	199
9.2 一致性测试	199
9.2.1 一致性测试的目的和内容	199
9.2.2 一致性测试的方法	200
9.2.3 一致性测试的原理	200
9.2.4 一致性测试的系统模型	202
9.3 实时性测试	203
9.3.1 递交时间测试	203
9.3.2 时钟同步精度测试	204
9.3.3 网络吞吐量测试	205
9.3.4 非实时通信带宽测试	206
9.3.5 冗余恢复时间测试	206
9.4 互可操作性测试	206
9.4.1 互操作测试系统结构	206
9.4.2 互操作测试内容	207
9.4.3 EPA 互操作测试的实施	209
9.5 小结	209
参考文献	209

第 10 章 EPA 组态	211
10.1 EPA 系统组态要求	211
10.2 EPA 组态软件概述	212
10.2.1 组态概念	212
10.2.2 软件概述	214
10.3 EPA 图形化组态与物理映射	215
10.3.1 主界面说明	215
10.3.2 设备管理	219
10.3.3 设备详细信息访问	229
10.3.4 控制策略组态	231
10.3.5 时间组态	235
10.3.6 功能安全	236
10.3.7 信息保存	236
10.3.8 应用实例	237
10.4 EPA 通信在线监控与诊断	241
10.5 小结	243
参考文献	243
第 11 章 基于 EPA 的控制系统的实际应用	244
11.1 基于 EPA 系统在华东制药的工程应用	244
11.1.1 工艺简介	244
11.1.2 系统的安装布置	245
11.1.3 系统控制方案实施与应用	247
11.2 基于 EPA 的系统在安全适用场合的应用	248
11.3 小结	250

第 1 章 绪 论

1.1 控制系统发展回顾

信息技术的飞速发展,引起了工业自动化系统结构的深刻变革。信息交换的范围正迅速覆盖从工厂的管理、控制到现场设备的各个层次,并逐步形成了全分布式网络集成自动化系统和以此为基础的企业信息系统。现场总线系统就是顺应信息技术的发展趋势和适应工业控制系统的分散化、网络化、智能化发展方向而发展起来的新技术,它的出现和发展已成为全球工业自动化技术的热点之一,受到全世界工业界的普遍重视^[1~5]。

自动控制系统的发展,经历了直接控制、集中控制、集散控制系统的过程。计算机、通信、网络等技术的发展使自动控制技术的发展有了更加广阔的空间。电力系统自动控制水平也对信息交换的速度和质量提出了更高要求。纵观控制系统的发展史,不难发现,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,最终在用户需求和市场竞争两大外因的推动下占领市场的主导地位,现场总线和现场总线控制系统的产生也不例外。自动控制系统发展经历了以下几个过程^[1~7]：

1) 模拟仪表控制系统

模拟仪表控制系统于 20 世纪六七十年代占主导地位。早期仪表与调节装置是机械式的,如膨胀式温度计、弹簧管式压力计和用于蒸汽机的飞球式调节器,其显著缺点是模拟信号精度低、易受干扰。

2) 集中式数字控制系统

集中式数字控制系统于 20 世纪七八十年代占主导地位。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。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、控制机时的选择上可以统一调度和安排;其缺点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,当系统任务增加时,控制器的效率和可靠性将急剧下降。

进入 20 世纪后,工业生产的规模开始扩大,需要将分散在现场的机械式仪表集中起来,于是就出现了有作为辅助能源的液动调节器,当时是采用油压的方式进行工作的,但由于油容易渗漏和发生火灾,再加上不能远距离调节,所以不久又出现了用压缩空气作为辅助能源的气动仪表与调节器,这样就出现了将检测、显示和

调节集中在一起的气动基地式仪表,后来为了便于集中在仪表室进行监控而又生产出气动单元组合仪表。集中式数字控制系统图例如图 1.1 所示。

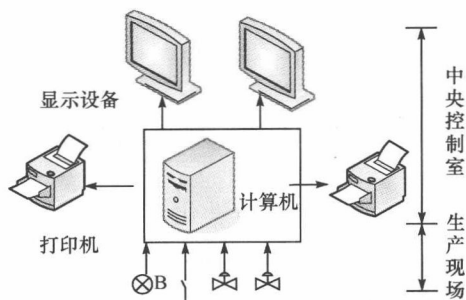


图 1.1 集中式数字控制系统

3) 集散控制系统

集散控制系统(distributed control system, DCS) 于 20 世纪八九十年代占主导地位。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,若干台下位机下放分散到现场实现分布式控制,各上下位机之间用控制网络互连以实现相互之间的信息传递。因此,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。在 DCS 中,分布式控制思想的实现正是得益于网络技术的发展和运用,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连和信息共享,因此 DCS 从该角度而言实质是一种封闭专用的、不具可互操作性的分布式控制系统,并且 DCS 造价昂贵。在这种情况下,用户对网络控制系统提出了开放化和降低成本的迫切要求。DCS 的信息采用一条信息线路进行传输。如果该条线路瘫痪,那么所有监控的数据将全部丢失。DCS 采用了多级分层网络结构、点对点的接线方式。它集多种功能于一台计算机上,无论是软件系统还是硬件系统都显得十分庞大。多种功能往往需要多实时任务去完成,因而效率不高。DCS 大多为模拟数字混合系统,尚未形成从测控设备到操作控制计算机的完整网络。DCS 的层次结构如图 1.2 所示,DCS 的体系结构如图 1.3 所示。

4) 现场总线控制系统

现场总线控制系统(fieldbus control system, FCS) 是利用现场总线这一开放的、具有可互操作的网络将现场各控制器及仪表设备互连来构成的,同时控制功能彻底下放到现场,降低了安装成本和维护费用。因此,FCS 实质是一种开放的、具可互操作性的、彻底分散的分布式控制系统,已经成为 21 世纪控制系统的主流产品。FCS 控制系统如图 1.4 所示。

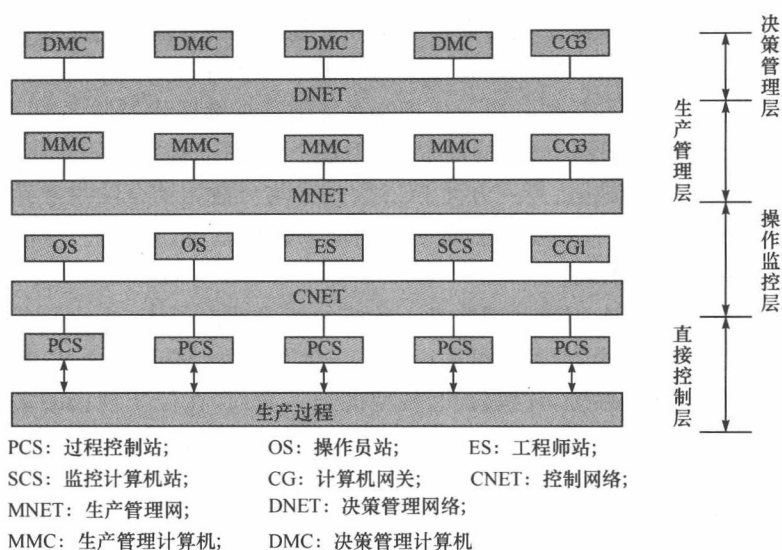


图 1.2 DCS 的层次结构图

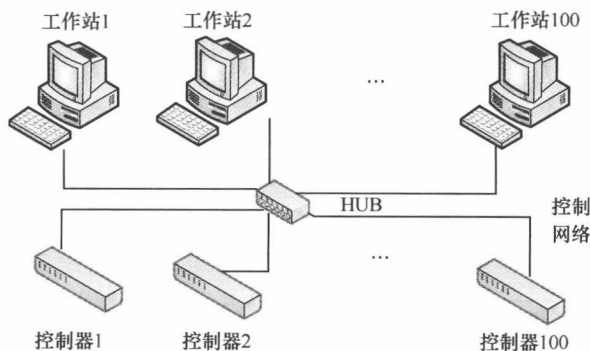


图 1.3 DCS 的体系结构图

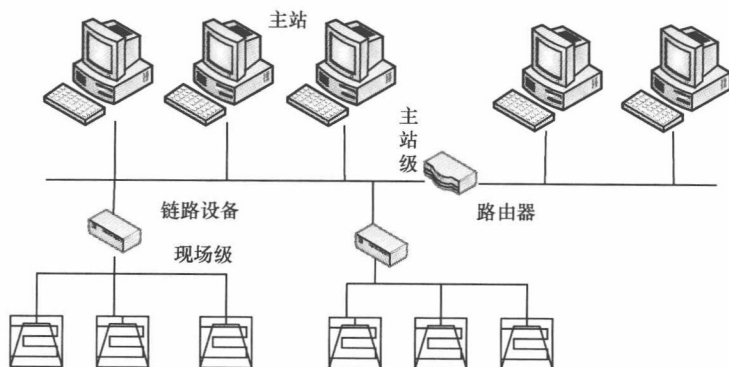


图 1.4 现场总线控制系统

“现场总线技术”实际上是将安装在工业过程现场的智能自动化仪表和装置与设置在控制室内的仪表和控制设备连接起来的一种数字化、串行、双向、多站的通信网络技术。基于这种总线的新一代控制系统被誉为第四代控制系统,即 FCS 一方面突破了 DCS 专用通信网络的局限,采用基于公开化、标准化的解决方案,克服了封闭系统所造成的缺陷;另一方面 FCS 将集中与分散相结合的集散系统变成了新型全分布式结构,把控制功能彻底下放到现场。可以说,开放性、分散性与数字通信是 FCS 最显著的特征。

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自动控制系统。简而言之,它把单个分散的测量控制设备变成网络节点,以现场总线为纽带,把它们连接成可以相互沟通信息、共同完成自控任务的网络系统与控制系统。正如众多分散的计算机被网络连接在一起,它给自动化领域带来的变化使计算机的功能、作用发生了变化。现场总线则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。传统的 DCS 系统结构和 FCS 体系结构如图 1.5 所示。

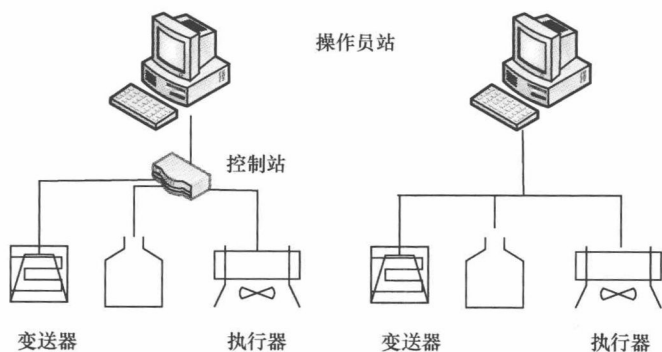


图 1.5 传统的 DCS 系统结构和 FCS 体系结构

1.2 工业控制网络

工业控制网络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。

控制室和现场仪表之间的信号传输经历了以 $4\sim 20\text{mA}$ 为代表的模拟信号,以内部数字信号和 RS232、RS485 为代表的数字通信,以控制网络(包括现场总线、

工业以太网、工业无线)为代表的网络传输三个阶段,每个阶段都伴随着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构成了企业综合自动化体系的核心技术和核心部件,并贯穿了整个企业综合自动化系统^[8~15](见图 1.6)。

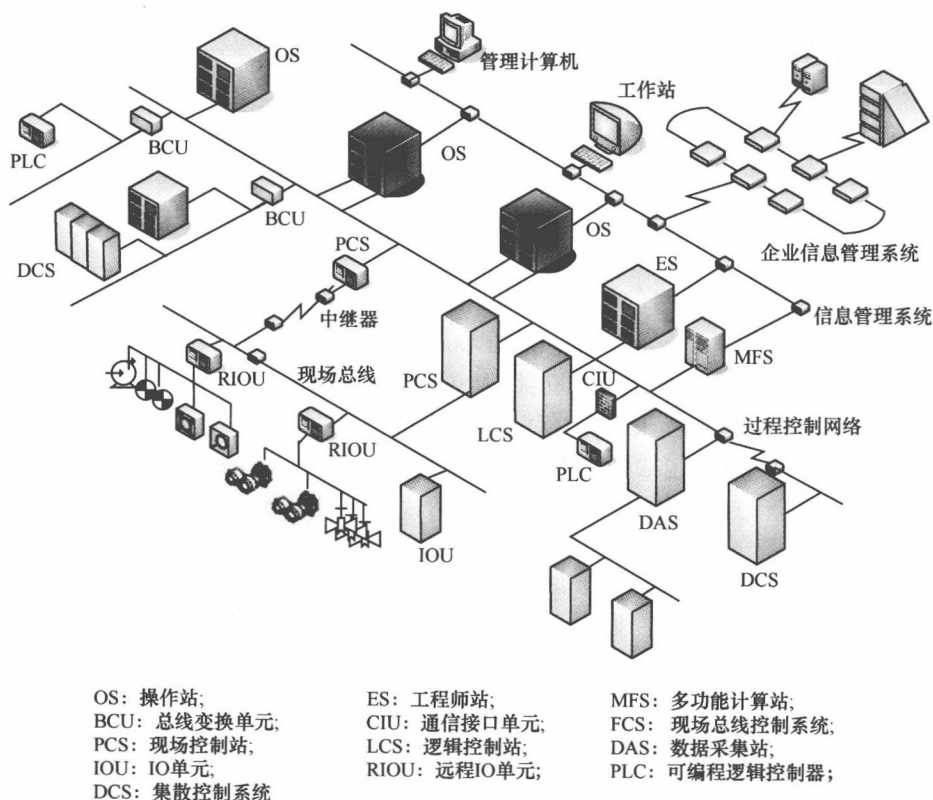


图 1.6 企业综合自动化系统网络架构图

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 DCS、PLC(可编程逻辑控制器)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

叫现场总线。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

过程控制网又叫过程监控网,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下载。

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、网络可用性有比较高的要求。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。为了确保信息传输及时可靠,工业控制网络对通信确定性、实时性、可靠性与可用性提出非常高的要求,同时对于过程控制网还提出了安全性的要求。

用于工业自动化系统的网络通信技术来源于 IT 信息技术的计算机网络技术,但是又不同于一般的计算机网络通信,这是因为 IT 网络通信是以传递信息为最终目的,而工业控制网络传递信息是以引起物质或能量的运动为最终目标。

正因为如此,工业控制网络与用于商业的网络通信技术有很大不同,其性能指标主要是实时性、确定性、可靠性和可用性^[2,5,7~17]:

1) 实时性

系统的实时性(real time)的含义是指对于某一给定任务而言,系统必须在一

个较小的时间内完成该任务的处理。简单理解来说,实时性就意味着系统工业网络必须要“快”。

对于工业自动化系统来说,目前根据不同的应用场合,将实时性要求划分为三个范围:信息集成和较低要求的过程自动化应用场合,实时响应时间要求是 100ms 或更长;绝大多数的工厂自动化应用场合实时响应时间的要求为 5~10ms;对于高性能的同步运动控制应用,特别是在 100 个节点下的伺服运动控制应用场合,实时响应时间要求低于 1ms,同步传送和抖动小于 $1\mu\text{s}$ 。

工业控制网络的实时性还规定了许多技术指标,如交付时间、吞吐量、时间同步、时间同步精度以及冗余恢复时间等实时性参数,具体可参见 IEC 61784-1—2010、IEC 61784-2—2010 等国际标准。

2) 确定性

工业控制网络的确定性主要用于描述系统可预测的响应时间和时延,即网络中任意两节点通信,从信息发送到信息接收之间全部延迟的最大时间是确定的。主要表现为任务(如功能块的执行)在时间上是可以预测的,要求最大值是可预知的,并小于一定值。由于以太网采用 CSMA/CD 介质访问方式,使得从根本上讲传统以太网是不确定的,这也是最初阻碍以太网进入工业控制领域的主要障碍。随着全双工交换式以太网的出现,传统以太网不确定性的缺点已经大大减小,但是在某些高速控制系统特别是运动控制系统中,交换式以太网的确定性仍然不能满足系统要求。

3) 可靠性

工业控制网络的可靠性是网络系统在一定时间内、在一定条件下无故障地执行指定功能的能力或可能性。工业控制网络的可靠性和实时性也是紧密相关的,如果信息传输的可靠性降低,接收到的信息错误可能性较大,必然造成信息的多次重传,接收节点可能无法及时地获取正确信息,从而造成实时性无法保证。另外,工业现场的环境十分恶劣,噪声干扰十分严重,大大降低了网络的可靠性,这就需要有合适的抗干扰措施和差错控制技术降低传输错误,保证系统可靠运作。

4) 可用性

工业控制网络的可用性是在要求的外部资源得到保证的前提下,在规定的条件下和规定的时刻或时间区间内处于可执行规定功能状态的能力。它是产品可靠性、维修性和维修保障性的综合反映。

与普通商用网络中传输的数据不同,在工业控制网络中,需要传输的信息主要分为三大类:

(1) 突发性实时信息,如报警信息、控制器之间的互锁信息等突发性数据。

(2) 周期性实时信息、周期性采样信息的传送等,在系统中以一定的周期时间出现具有可预测性。如过程数据要求每个周期实时采样,并传递到控制器,控制器