

现场总线与 工业以太网应用

郭其一 黄世泽 薛吉 屠旭慰 著



科学出版社

现场总线与工业以太网应用

郭其一 黄世泽 薛吉 屠旭慰 著

科学出版社

北京

内 容 简 介

本书以国际标准的几种主流现场总线为背景,介绍了有关现场总线产生的背景、基础、通信协议、网络体系结构以及产品和应用等方面的内容。主要内容包括:现场总线的基本概念,工业通信相关基础知识,Modbus、Profibus-DP、Modbus/TCP 的产品开发过程,组态软件及系统构建方法。

本书内容较为完整和丰富,旨在帮助从事自动化和仪表领域的技术人员和相关专业的高年级本科生和研究生更加深入地了解现场总线技术、开阔眼界、增加知识面,也可作为高等院校电气工程类专业的教学参考书。

图书在版编目(CIP)数据

现场总线与工业以太网应用/郭其一等著. —北京:科学出版社,2016.3
ISBN 978-7-03-047539-8

I. ①现… II. ①郭… III. ①总线-自动控制系统 ②工业企业-以太网
IV. ①TP273 ②TP393.11

中国版本图书馆 CIP 数据核字(2016)第 044372 号

责任编辑:张海娜 高慧元 / 责任校对:郭瑞芝

责任印制:张 倩 / 封面设计:蓝正设计

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

*

2016年3月第一版 开本:720×1000 1/16

2016年3月第一次印刷 印张:16 1/4

字数:317 000

定价:98.00元

(如有印装质量问题,我社负责调换)

前 言

以计算机(computer)、通信(communication)和控制(control)为代表的 3C 技术迅速发展,使得网络集成信息自动化正在迅速应用到现场设备、控制、管理和市场的各个层次,迅速进入工业制造、工业流程、环境工程、民用工程等应用领域。现场总线是将自动化最底层的现场控制器和现场智能仪表设备互连的实时控制通信网络,它遵循 ISO/OSI 开放系统互连参考模型的全部或部分通信协议。现场总线是自动化领域技术发展的热点之一,它的出现标志着工业控制技术领域又一新时代的开始。

现场总线技术是用于现场仪表与控制系统和控制室之间的一种全分散、全数字化、智能、双向、互连、多变量、多点、多站的串行通信技术,被誉为自动化领域的局域网,它是计算机技术、通信技术、控制技术的集成。现场总线技术使控制系统向着分散化、智能化、网络化方向发展,使控制技术与计算机及网络技术的结合更为紧密。基于开放通信协议标准的现场总线,为控制网络与信息网络的连接提供了便利,因而对控制网络与信息网络的融合和集成起到了积极的促进作用。

本书以国际标准的几种主流现场总线为背景,介绍有关现场总线产生的背景、基础、通信协议、网络体系结构以及产品和应用等方面的内容。全书共 6 章。第 1 章介绍现场总线的基本概念、产生背景、发展历程以及发展趋势,并简要介绍几种主流现场总线。第 2 章详细介绍工业通信相关基础知识,包括传输介质、通信方式、网络拓扑等。第 3~5 章分别着重介绍 Modbus、Profibus-DP、Modbus/TCP 的产品开发过程,包括基本协议介绍、硬件开发和软件开发等。第 6 章介绍组态软件及系统,详细分析 Modbus、Profibus-DP、Modbus/TCP 的组态软件接入方法,最后介绍一个现场总线控制系统实例,以便读者深入研究。

通过阅读本书,读者可以详细了解现场总线技术,并根据本书的内容建立一个简单的基于现场总线的控制系统。本书是在对相关参考资料参考、引用和整理的基础上编写而成的,在此感谢所引用资料或文献的作者。感谢浙江中凯科技股份有限公司为本书的应用章节提供的产品和案例。

由于作者的学识和实践经验所限,掌握的资料也不够全面,对现场总线技术的研究还有待深入,加之现场总线技术发展迅猛,新技术层出不穷,书中疏漏之处在所难免,恳请广大读者指正和赐教。

目 录

前言

第 1 章 绪论	1
1.1 现场总线	1
1.1.1 现场总线的基本概念	1
1.1.2 现场总线的发展历程	2
1.1.3 主流现场总线介绍	3
1.2 工业以太网	8
1.2.1 工业以太网的基本概念	8
1.2.2 工业以太网的发展历程	9
1.3 标准介绍	20
1.3.1 IEC61158	20
1.3.2 IEC62026	23
1.3.3 IEC61784	23
1.3.4 现场总线中国标准	25
1.4 现场总线与工业以太网技术的发展趋势	26
1.4.1 现场总线技术的发展趋势	26
1.4.2 工业以太网技术的发展趋势	27
第 2 章 工业通信基础知识	30
2.1 传输介质	30
2.1.1 有线介质	30
2.1.2 无线介质	35
2.2 数字编码方式	37
2.3 通信方式	41
2.3.1 并行通信与串行通信	41
2.3.2 同步传输与异步传输	42
2.3.3 单工、半双工与全双工通信	45
2.4 网络拓扑	46
2.4.1 总线拓扑	46
2.4.2 星形拓扑	47
2.4.3 树形拓扑	48

2.4.4	环形拓扑	49
第3章	Modbus 产品开发	51
3.1	基本介绍	51
3.1.1	协议介绍	51
3.1.2	模式分类	53
3.2	产品开发	59
3.2.1	硬件	59
3.2.2	软件	61
第4章	Profibus-DP 产品开发	64
4.1	Profibus 基本介绍	64
4.1.1	组织	64
4.1.2	通信协议	64
4.1.3	传输技术	65
4.2	Profibus-DP 基本原理	66
4.2.1	基本特征	66
4.2.2	通信协议	68
4.2.3	DP 报文解析	69
4.3	从站产品开发	83
4.3.1	从站分类	83
4.3.2	从站设计方案	86
4.3.3	硬件开发	87
4.3.4	软件开发	94
4.3.5	GSD 文件	118
4.3.6	组网配置	121
第5章	Modbus/TCP 产品开发	150
5.1	基本介绍	150
5.1.1	组织	150
5.1.2	标准	150
5.1.3	基本特征	150
5.1.4	通信协议	151
5.1.5	报文解析	151
5.2	产品开发	152
5.2.1	从站分类	152
5.2.2	从站设计方案	155
5.2.3	硬件	159

5.2.4	软件	160
5.2.5	开发过程中注意事项	167
5.2.6	报文分析	167
5.2.7	组网配置	172
第6章	组态软件及系统	184
6.1	组态软件介绍	184
6.2	三维力控软件介绍	185
6.3	组态软件开发	186
6.3.1	Modbus 现场总线的组态软件接入	186
6.3.2	Profibus-DP 现场总线的组态软件接入	199
6.3.3	Modbus/TCP 工业以太网组态软件接入	221
6.4	现场总线控制系统实例	239
6.4.1	项目概述	239
6.4.2	项目总体设计方案	240
6.4.3	项目具体设计方案	243
6.4.4	项目实施及运行	248
	参考文献	249

第 1 章 绪 论

1.1 现场总线

20 世纪 80 年代中期产生的现场总线,主要特征是以全数字、双向传输、多分支结构的通信控制总线连接智能现场设备,使工业控制系统向分散化、网络化和智能化方向发展,从而使工业控制系统的体系结构和功能结构产生重大变革。如果说计算机网络把人类引进了信息时代,那么现场总线则让自动控制系统加入到信息网络的行列,成为企业信息网络的底层,使企业信息沟通的覆盖范围一直延伸到生产现场。

1.1.1 现场总线的基本概念

关于现场总线的定义有很多种。它原本是指现场设备之间公用的信号传输线。后来又被定义为一种应用于生产现场,在现场设备之间、现场设备与控制装置之间实行双向、串行、多节点数字通信的技术。具体来说,它以测量控制设备作为网络节点,以双绞线等传输介质为纽带,把位于生产现场、具备数字计算和数字通信能力的测量控制设备连接成网络系统,按公开、规范的通信协议,在多个测量控制设备之间,以及现场设备与远程监控计算机之间,实现数据传输与信息交换,形成适应各种应用需要的自动控制系统。随着技术内容的不断发展和更新,现场总线已经成为控制网络技术的代名词。它使自控设备连接为控制网络,并与计算机网络沟通连接,使控制网络成为信息网络的重要组成部分。

现场总线系统既是一个开放的数据通信系统、网络系统,又是一个可以由现场设备实现完整控制功能的全分布控制系统。它作为现场设备之间信息沟通交换的联系纽带,把挂接在总线上、作为网络节点的设备连接为实现各种测量控制功能的自动化系统,实现如 PID 控制、补偿计算、参数修改、报警、显示、监控、优化及控管一体化的综合自动化功能。这是一项以数字通信、计算机网络、自动控制为主要内容的综合技术^[1,2]。

现场总线的主要特点如下:

(1) 开放性。现场总线为开放式互连网络,其技术和标准都是公开的,所有制造商都必须遵循。这样用户可以自由集成不同制造商的通信网络,能与不同的控制系统形成互连。

(2) 布线简单。现场总线的最大革命是布线方式的革命。现场总线系统的接

线十分简单,由于一对双绞线或一条电缆上通常可挂接多个设备,因而电缆、端子、槽盒、桥架的用量大大减少,连线设计与接头校对的工作量也大大减少。当需要增加现场控制设备时,无需增设新的电缆,可就近连接在原有的电缆上,因此最小化的布线方式和最大化的网络拓扑使得系统的接线成本和维护成本大大降低。

(3) 实时性。现场总线的实时性是为了满足现场控制和现场数据采集的要求。在确保数据传输可靠性和稳定性的前提下,现场总线应具备较高的传输速率和传输效率。

(4) 可靠性。由于现场总线设备的智能化、数字化,与模拟信号相比,它从根本上提高了测量与控制的准确度,减少了传送误差。同时,由于系统的结构简化,现场设备内部功能加强,设备之间连线减少,这都减少了信号的往返传输,提高了系统的工作可靠性。而且,现场总线一般都具有一定的抗干扰能力,同时具备一定的诊断能力,可最大限度地保护整个系统,并快速地查找、更换故障节点^[2]。

1.1.2 现场总线的发展历程

20世纪50年代以前,由于当时的生产规模较小,检测控制仪表尚处于发展的初级阶段,所采用的是直接安装在生产设备上、只具备简单测控功能的基地式气动仪表,其信号仅在本仪表内起作用,一般不能传送给别的仪表或系统,即各测控点只能成为封闭状态,无法与外界沟通信息,操作人员只能通过生产现场的巡视,了解生产过程的状况。

在过程控制领域,从20世纪50年代至今,随着生产规模的扩大,操作人员需要综合掌握多点的运行参数与信息,需要同时按多点的信息实行操作控制,于是出现了气动、电动系列的单元组合式仪表,出现了集中控制室。生产现场各处的参数通过统一的模拟信号,如 $0\sim 10\text{mA}$ 、 $4\sim 20\text{mA}$ 的直流电流信号, $1\sim 5\text{V}$ 直流电压信号等,送往集中控制室,在控制盘上连接。操作人员可以坐在控制室纵观生产流程各处的状况,可以把各单元仪表的信号按需要组合成复杂控制系统^[3]。

传统模拟控制系统采用一对一的物理连接,即模拟信号的传递需要一对一的物理连接,信号变化缓慢,提高计算速度与精度的开销、难度都较大,信号传输的抗干扰能力也较差,于是人们开始寻求用数字信号取代模拟信号,出现了直接数字控制系统(DDC)。由于当时的数字计算机技术尚不发达,价格昂贵,人们企图用一台计算机取代控制室几乎所有的仪表盘,出现了集中式数字控制系统。但由于当时数字计算机的可靠性还较差,一旦计算机出现某种故障,就会造成所有控制回路瘫痪、生产停产的严重局面,这种危险集中的系统结构很难为生产过程所接受。

随着计算机功能的不断增强,价格急剧降低,计算机与计算机网络系统得到了迅速发展,出现了数字调节器、可编程控制器(PLC)以及由多个计算机递阶构成的

集中分散相结合的集散控制系统(DCS)。在DCS中,测量变送仪表一般为模拟仪表,它属于模拟数字混合系统。这种系统在功能、性能上较模拟仪表、集中式数字控制系统有了很大进步,可在此基础上实现装置级、车间级的优化控制。但是,在DCS形成的过程中,由于设备之间采用传统的一对一连线,用电压、电流的模拟信号进行测量控制,或采用自成体系的封闭式集散系统,难以实现设备之间以及系统与外界之间的信息交换,使自动化系统成为了“信息孤岛”。再者,各厂家的产品自成系统,不同厂家的设备不能互连在一起,难以实现互换与互操作,组成更大范围信息共享的网络系统存在很大困难。

要实现整个企业的信息集成,实施综合自动化,就要构建运行在生产现场、性能可靠、造价低廉的工厂底层网络,完成现场自动化设备之间的多点数字通信,实现底层现场设备之间以及生产现场与外界的信息交换。现场总线就是在这种实际需求驱动下应运而生的。它作为现场设备之间互连的控制网络,沟通了生产过程现场控制设备之间及其与更高控制管理层网络之间的联系,克服了DCS中采用专用网络所造成的缺陷,把基于封闭、专用的解决方案变成了基于公开化、标准化的解决方案。把来自不同厂商而遵守同一协议规范的自动化设备,通过现场总线网络连接成系统,实现综合自动化的各种功能,同时把DCS的模拟数字混合系统结构,变成了新型的全分布式网络系统结构,为彻底打破自动化系统的信息孤岛僵局创造了条件。

现场总线系统的现场设备在不同程度上都具有数字计算和数字通信能力。借助现场设备的计算、通信能力,在现场就可进行多种复杂的控制计算,形成真正分散在现场的完整的控制系统,提高了控制系统运行的可靠性。可借助现场总线控制网络,以及与之有通信连接的其他网络,实现异地远程自动控制,如操作远在数百公里之外的电气开关等;还可提供传统仪表所不能提供的如设备资源、阀门开关动作次数、故障诊断等信息,便于操作人员更好、更深入地了解生产现场和自控设备的运行状态^[4,5]。

1.1.3 主流现场总线介绍

近年来,欧洲、北美、亚洲的许多国家都投入巨额资金与人力,研究开发现场总线技术,出现了百花齐放、兴盛发展的态势。据说,世界上已出现各式各样的现场总线100多种,其中宣称为开放型现场总线的就有40多种^[6]。有些已经在特定的应用领域显示了各自的特点和优势,表现了较强的生命力。比较流行的主要有基金会现场总线(FF)、过程现场总线(Profibus)、设备网(DeviceNet)、LonWorks等现场总线。

1. 基金会现场总线

基金会现场总线(foundation fieldbus, FF)是在过程自动化领域得到广泛支持和具有良好发展前景的技术。其前身是以美国 Fisher-Rosemount 公司为首,联合 Foxboro、横河、ABB、西门子等 80 家公司制定的 ISP 协议,以及以 Honeywell 公司为首、联合欧洲等地的 150 家公司制定的 WorldFIP 协议。屈于用户的压力,这两大集团于 1994 年 9 月合并,成立了现场总线基金会,致力于开发出国际上统一的现场总线协议。它以 ISO/OSI 开放系统互连模型为基础,取其物理层、数据链路层、应用层为 FF 通信模型的相应层次,并在应用层上增加了用户层。

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 31.25kbit/s,通信距离可达 1900m(可加中继器延长),可支持总线供电,支持本征安全防爆环境。H2 的传输速率为 1Mbit/s 和 2.5Mbit/s 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。

基金会现场总线的物理媒介的传输信号采用曼彻斯特编码,每位发送数据的中心位置或是正跳变或是负跳变。正跳变代表“0”,负跳变代表“1”,从而使串行数据位流中具有足够的定位信息,以保持发送双方的时间同步。接收方既可根据跳变的极性来判断数据的“1”“0”状态,也可根据数据的中心位置精确定位。

为满足用户需要,Honeywell、Ronan 等公司已开发出可完成物理层和部分数据链路层协议的专用芯片,许多仪表公司已开发出符合 FF 协议的产品,H1 总线已通过 α 测试和 ρ 测试,完成了由 13 个不同厂商提供设备而组成的 FF 现场总线工厂试验系统。H2 总线标准也已形成。1996 年 10 月,在芝加哥举行的 ISA96 展览会上,由现场总线基金会组织实施,向世界展示了来自 40 多家厂商的 70 多种符合 FF 协议的产品,将这些分布在不同楼层展览大厅不同展台上的 FF 展品,用醒目的橙红色电缆,互连为 7 段现场总线演示系统,各展台现场设备之间可实地进行现场互操作,展现了基金会现场总线的成就与技术实力^[7-9]。

2. 过程现场总线

Profibus(process fieldbus)是一种具有广泛应用范围的、开放的数字通信系统,根据应用特点,主要分为 Profibus-DP、Profibus-FMS、Profibus-PA 三种类型。

DP 型总线用于分散外设间的高速传输,适合于加工自动化领域的应用;FMS 型总线为现场信息规范,适用于纺织、楼宇自动化、可编程控制器、低压开关等一般自动化;而 PA 型则是用于过程自动化的总线类型,它遵从 IEC1158-2 标准。

Profibus 采用了 OSI 模型的物理层、数据链路层,由这两部分形成了其标准第一部分的子集。DP 型隐去了第 3~7 层,增加了直接数据连接拟合作为用户接口,

FMS 型只隐去第 3~6 层,采用了应用层作为标准的第二部分,PA 型的传输技术遵从 IEC1158-2(H1)标准,可实现总线供电与本征安全防爆。

Profibus 支持单主站、多主站系统,主站有对总线的控制权,可主动发送信息。对多主站系统来说,主站之间采用令牌方式传递信息,得到令牌的站点可在一个预定时间内拥有总线控制权,并事先规定好令牌在各主站中循环一周的最长时间。按 Profibus 的通信规范,令牌在主站之间按地址编号顺序,沿上行方向进行传递。主站通过令牌得到控制权后,按主从方式与从站交互数据,实现点对点通信。主站向所有站点广播信息,或有选择地向一组站点广播,而从站并不需要应答^[10-12]。

3. 设备网

在现代的控制系统中,不仅要求现场设备完成本地的控制、监视、诊断等任务,还要能通过网络与其他控制设备及 PLC 进行对等通信,因此现场设备多设计成内置智能式。基于这样的现状,美国 Rockwell Automation 公司于 1994 年推出了 DeviceNet 网络,实现低成本高性能的工业设备的网络互连。

DeviceNet 是一种低成本的通信连接,它将工业设备连接到网络,从而免去了昂贵的硬接线。DeviceNet 又是一种简单的网络解决方案,在提供多供货商同类部件间可互换性的同时,减少了配线和安装工业自动化设备的成本和时间。DeviceNet 的直接互连性不仅改善了设备间的通信,同时提供了相当重要的设备级诊断功能,这是通过硬接线 I/O 接口很难实现的^[13,14]。

DeviceNet 具有如下特点:

(1) DeviceNet 基于 CAN 总线技术,它可连接开关、光电传感器、阀组、电动机启动器、过程传感器、变频调速设备、固态过载保护装置、条形码阅读器、I/O 和人机界面等,传输速率为 125~500kbit/s,每个网络的最大节点数是 64 个,干线长度 100~500m。

(2) DeviceNet 使用的通信模式是:生产者/消费者(producer/consumer)。该模式允许网络上的所有节点同时存取同一源数据,网络通信效率更高;采用多信道广播信息发送方式,各个消费者可在同一时间接收到生产者所发送的数据,网络利用率更高。“生产者/消费者”模式与传统的“源/目的”通信模式相比,前者采用多信道广播式,网络节点同步化,网络效率高;后者采用应答式,如果要向多个设备传递信息,则需要对这些设备分别进行“呼”“应”通信,即使是同一信息,也需要制造多个信息包,这样,增加了网络的通信量,网络响应速度受限制,难以满足高速的、对时间要求苛刻的实时控制。

(3) 设备可互换性。各个销售商所生产的符合 DeviceNet 网络和行规标准的简单装置(如按钮、电动机启动器、光电传感器、限位开关等)都可以互换,为用户提供了灵活性和可选择性。

(4) DeviceNet 网络上的设备可以随时连接或断开,而不会影响网络上其他设备的运行,方便维护和减少维修费用,也便于系统的扩充和改造。

(5) DeviceNet 网络上的设备安装比传统的 I/O 布线更加节省费用,尤其是当设备分布在几百米范围内时,更有利于降低布线安装成本。

现场总线技术具有网络化、系统化、开放性的特点,需要多个企业相互支持、相互补充来构成整个网络系统。为便于技术发展和企业之间的协调,统一宣传推广技术和产品,通常每一种现场总线都有一个组织来统一协调。DeviceNet 总线的组织机构是开放式 DeviceNet 供货商协会(Open DeviceNet Vendors Association, ODVA)。它是一个独立组织,管理 DeviceNet 技术规范,促进 DeviceNet 在全球的推广与应用。

ODVA 实行会员制,会员分供货商会员(vendor member)和分销商会员(distributor member)。ODVA 现有供货商会员 310 个,其中包括 ABB、Rockwell-PhoenixContact、Omron、Hitachi、Cutler-Hammer 等几乎所有世界著名的电气和自动化组件生产商。

ODVA 的作用是帮助供货商会员向 DeviceNet 产品开发者提供技术培训、产品一致性试验工具和试验,支持成员单位对 DeviceNet 协议规范进行改进;出版符合 DeviceNet 协议规范的产品目录,组织研讨会和其他推广活动,帮助用户了解掌握 DeviceNet 技术;帮助分销商开展 DeviceNet 用户培训和 DeviceNet 专家认证培训,提供设计工具,解决 DeviceNet 系统问题^[15]。

4. LonWorks

LonWorks 是又一具有强劲实力的现场总线技术,它是由美国 Echelon 公司推出并与 Motorola、Toshiba 公司共同倡导,于 1990 年正式公布而形成的。它采用了 ISO/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 300bit/s 至 1.5Mbit/s 不等,直接通信距离可达到 2700m(不加中继器),支持双绞线、同轴电缆、光纤、射频、红外线、电源线等多种通信介质,被誉为通用控制网络。

LonWorks 技术所采用的 LonTalk 协议被封装在称为 Neuron 的芯片中并得以实现。集成芯片中有 3 个 8 位 CPU,一个用于完成开放互连模型中第 1、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、函数路径选择、软件计量、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,如 Motorola 公司生产的神经元集成芯片 MC143120E2 就包含了 2KB RAM 和 2KB EEPROM。

LonWorks 公司的技术策略是鼓励各 OEM 开发商运用 LonWorks 技术和神经元芯片,开发自己的应用产品。据称目前已有 4000 多家公司在不同程度上采用 LonWorks 技术;1000 多家公司已经推出了 LonWorks 产品,并进一步组织起 LonMark 互操作协会,开发推广 LonWorks 技术与产品。为了支持 LonWorks 与其他协议和网络之间的互联与互操作,该公司正在开发各种网关,以便将 LonWorks 与以太网、FF、Modbus、DeviceNet、Profibus 等互联为系统。

另外,在开发智能通信接口、智能传感器方面,LonWorks 神经元芯片也具有独特的优势。

LonWorks 技术已经被美国暖通工程师协会(ASHRE)定为建筑自动化协议 BACNet 的一个标准。美国消费电子制造商协会已经通过决议,以 LonWorks 技术为基础制定了 EIA-709 标准。这样,LonWorks 已经建立了一套从协议开发、芯片设计、芯片制造、控制模块开发制造、OEM 控制产品、最终控制产品、分销、系统集成等一系列完整的开发、制造、推广、应用体系结构,吸引了数万家企业参与到这项工作中来,这对于一种技术的推广、应用有很大的促进作用。表 1.1 所示为对以上几种现场总线的性能作简单比较^[16-18]。

表 1.1 几种流行的现场总线比较

类型特性	FF	Profibus	DeviceNet	LonWorks
开发公司	Fisher-Rosemount 公司	西门子公司	Rockwell 公司	Echelon 公司
OSI 网络层次	1,2,7,(8)	1,2,7	1,2,7	1~7
通信介质	双绞线、同轴电缆和光纤	双绞线、光纤	双绞线、同轴电缆和光纤	双绞线、光纤、同轴电缆、无线和电力线
介质访问方式	令牌	令牌	带非破坏性逐位仲裁的载波侦听多址访问(CSMA/NBA)	可预测 P 坚持 CSMA (Predictive P-Persistent CSMA)
最大通信速率/(kbit/s)	31.25(H1) 100000(H2)	12000	500	1500
最大节点数	32	127	64	248
优先级	有	有	有	有
本征安全性	是	是	是	是
开发工具	有	有	有	有

1.2 工业以太网

随着社会的不断进步,工业自动化系统开始向分布式、智能化的实时控制方面发展,用户要求企业从现场控制层到管理层能实现全面的无缝信息集成,并提供一个开放的基础构架,这些都要求控制网络使用开放的、透明的通信协议,但是以前的系统往往无法满足这些要求,近年来国际工业控制领域的共同趋势是使用基于 IEEE802.3 和 TCP/IP 的网络技术,形成新型的基于以太网的网络控制技术,即工业以太网。

1.2.1 工业以太网的基本概念

工业以太网源于以太网而又不同于以太网。互联网及普通计算机网络采用的以太网技术原本并不适应控制网络和工业环境的应用需要。

所谓工业以太网,一般来讲是指技术上与商用以太网(IEEE802.3 标准)兼容,又针对工业应用采取了改进措施使其更加适用于工业场合。在产品的设计时,材质的选用、适用性、实时性、可靠性、互操作性和抗干扰性等方面能满足工业现场的需要^[19],其特点如下。

1. 实现高速、大数据量的实时、稳定传输

以太网能实现大数据量数据的交互,而快速以太网与交换式以太网技术的发展,给解决工业以太网的非确定性问题带来了新的契机,以太网的通信速率从 10M、100M 增大到如今的 1000M、10G,在数据吞吐量相同的情况下,通信速率的提高意味着网络负荷的减轻和网络传输延时的减小,即网络碰撞概率大大下降。其次,交换机迅速发展,可对网络上传输的数据进行过滤,使每个网段内节点间数据的传输只限在本地网段内进行,不占用其他网段的带宽,从而降低了所有网段和主干网的网络负荷。再次,全双工通信也避免了冲突的发生。因此工业以太网通信的实时性和稳定性大大提高。

2. Web 功能的集成

Web 功能的集成使用户可以通过以太网技术访问设备,如 HTTP、HTML 等。这样,只要借助互联网的标准技术可访问工业以太网设备,获得设备相关信息或者对有些信息进行配置修改。

3. 集成原有现场总线系统

工业以太网的出现,给原有的现场总线带来了一定的冲击,为了保护用户原有

投资,工业以太网必须能无缝集成原有现场总线系统,这一般都是通过网关实现,可通过网关将原先的现场总线系统接入不同的工业以太网系统中。

以工业以太网 Modbus/TCP 为例,如图 1.1 所示,网关把原有的 Modbus 网络接入 Modbus/TCP 网络,网关在 Modbus/TCP 网络中充当 Modbus/TCP 从站,在 Modbus 网络中则充当 Modbus 主站。

同样,其他工业以太网也可以通过相应的转换装置连接现场总线网络。

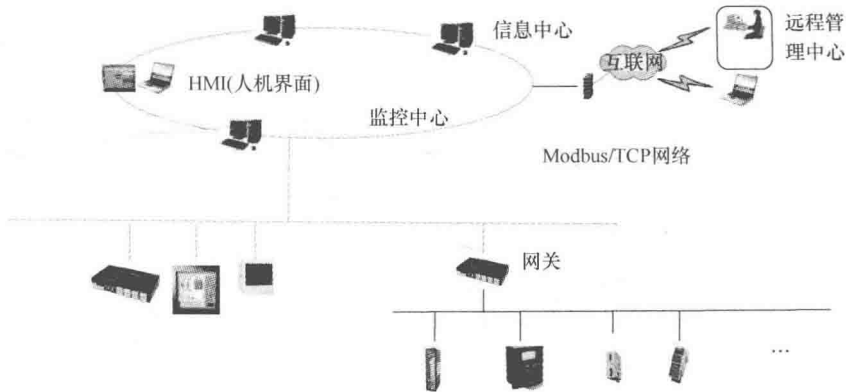


图 1.1 Modbus/TCP 网络

4. 时钟同步

IEEE 1588(网络测控系统精确时钟同步协议)最初由 Agilent Laboratories (安捷伦实验室)的 John Eidsen 以及来自其他公司和组织的 12 名成员开发,后来得到 IEEE 的赞助,并于 2002 年 11 月得到 IEEE 批准。

IEEE 1588 的基本功能是使分布式网络内的最精确时钟与其他时钟保持同步,它定义了一种精确时间协议 PTP(precision time protocol),用于对标准以太网或其他采用多播技术的分布式总线系统中的传感器、执行器以及其他终端设备中的时钟进行亚微秒级同步。目前,许多工业以太网都能实现符合 IEEE 1588 的时钟同步功能^[20]。

1.2.2 工业以太网的发展历程

在 20 世纪 70 年代中期,美国施乐公司提出了以太网这个新概念,通过以太网超过 100 个网站可以不需要预先知道对方站点的信息就可以以非常高的数据传输速率(在当时是非常高的速率)进行通信,通过约 1000m 的同轴电缆,数据传输速率从最初的 3Mbit/s 发展到后来的 10Mbit/s。

Robert M. Metcalfe 博士在 1976 年绘制了著名的工业以太网草图,并在这一年的 6 月的国家计算机会议提出了以太网。在这张图中最先描述了以太网的各部分

术语。从此以后其他术语开始在以太网的普及中得到应用。

随着科技的发展,带有冲突检测的载波侦听多路存取(CSMA/CD)的方法不断改进,从而形成一致而又强大的局域网技术。各种各样的措施改进了以太网技术,并且使以太网可以适应新的可能的技术。

以太网在 Internet 中的广泛应用,使得它具有技术成熟、软硬件资源丰富、性价比高等许多明显的优势,得到了广大开发商与用户的认同。今天,以太网已经属于成熟技术。

从实际应用状况分析,工业以太网的应用场合各不相同。它们有的作为工业应用环境下的信息网络,有的作为现场总线的高速(或上层)网段,有的是基于普通以太网技术的控制网络,而有的则是基于实时以太网技术的控制网络。不同网络层次、不同应用场合需要解决的问题,需要的特色技术内容各不相同。

以太网技术的发展和广泛应用,使其从办公自动化走向工业自动化。首先是通信速率的提高,以太网以 10M、100M 到现在的 1000M、10G,速率提高意味着网络负荷减轻和传输延时减少,网络碰撞概率下降;其次采用双工星形网络拓扑结构和以太网交换技术,使以太网交换机的各端口之间数据帧的输入和输出不再受 CSMA/CD 机制的制约,避免了冲突;再加上全双工通信方式使端口间两对双绞线(或两根光纤)上分别同时接收和发送数据,而不发生冲突。这样,全双工交换式以太网能避免因碰撞而引起的通信响应不确定性,保障通信的实时性。同时,由于工业自动化系统向分布式、智能化的实时控制方面发展,通信成为关键,用户对统一的通信协议和网络的要求日益迫切。这样,技术和应用的发展,使以太网进入工业自动化领域成为必然。所以工业以太网正在成为一种很有发展前途的现场控制网络^[21,22]。

1. 主流工业以太网介绍

随着现场总线应用领域的扩展和建立企业信息系统的需求,工业以太网在现场总线中迅速崛起并不断发展。目前,主流工业以太网主要有:现场总线基金会的高速以太网 HSE(high speed Ethernet)、控制网国际组织(ControlNet International, CI)和 ODVA 工业以太网 Ethernet/IP(Ethernet/industrial protocol)、Profibus 用户组织(Profibus Nutzer Organization, PNO)Profinet、Modbus-IDA、Modbus/TCP^[23,24]。

2. Modbus/TCP

工业以太网 Modbus/TCP 是由施耐德电气公司为首的 Modbus-IDA 组织推出,它基于标准的 TCP/IP 协议,定义了一个结构简单的、开放和广泛应用的传输协议,用于主从式通信。其网络结构如图 1.2 所示。

主要技术特征如下:

- (1) 拓扑形式,开放局域网络,符合 IEEE802.3。