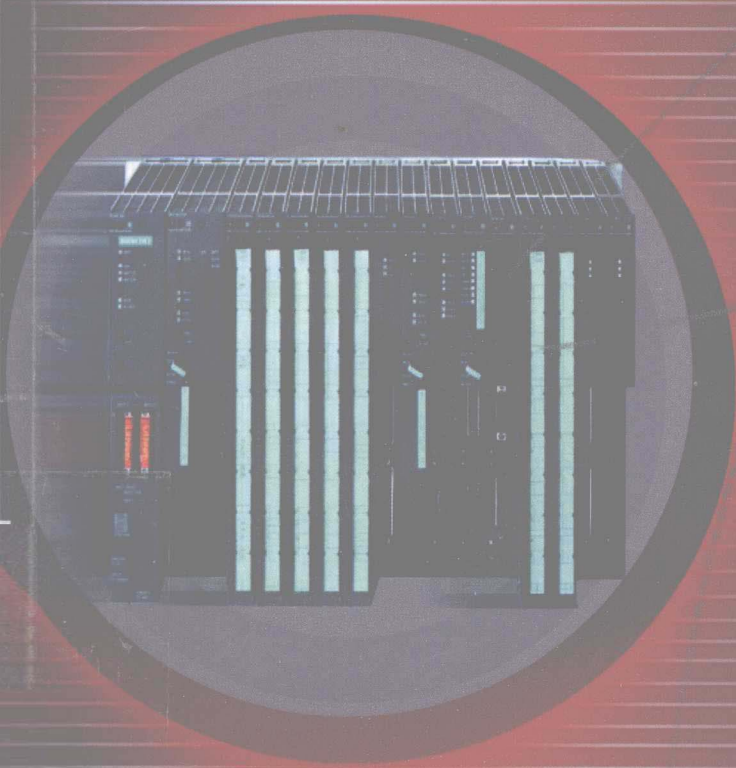


普通高等学校教材
西门子自动化产品培训用书
SIEMENS

S7-300/400 PLC 工业网络通信技术指南



SIEMENS

刘建昌 于洪磊 辛红 杜平 等编著

普通高等学校教材

西门子自动化产品培训用书

S7-300/400 PLC 工业网络 通信技术指南

刘建昌 于洪磊 辛 红 杜 平 等编著

机械工业出版社

本书从网络通信的实际应用出发,全面讲述了西门子公司的 S7-300/400 PLC 的工业网络通信技术,涵盖 MPI、工业以太网、PROFIBUS、AS-i 通信、点对点通信、与外部设备的串行通信以及网络路由功能。本书的特点是理论结合实例,讲解系统易懂、内容详实、方法简单实用。

同时书中的每个通信实例互为独立单元,图文并茂、条理清晰、深入浅出地阐述了通信协议的各个方面,便于初学者学习与运用。

本书既可作为高等院校工业自动化、电气工程、电工、机电一体化、计算机应用及相关专业高年级本科生和研究生可编程控制器等课程的教材,同时也可以作为广大从事电气、电工行业的研发工程师、专业技术人员以及正在学习 PLC 的专业人员的参考书或者培训教材。

图书在版编目 (CIP) 数据

S7-300/400 PLC 工业网络通信技术指南/刘建昌等编著. —北京:机械工业出版社, 2009. 5

普通高等学校教材. 西门子自动化产品培训用书

ISBN 978-7-111-26698-3

I. S… II. 刘… III. ①可编程序控制器—指南②工业控制计算机—计算机网络—计算机通信—指南 IV. TM571.6-62 TP273-62

中国版本图书馆 CIP 数据核字 (2009) 第 046195 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

策划编辑: 张俊红 责任编辑: 林 楨

版式设计: 霍永明 责任校对: 姜 婷

封面设计: 鞠 杨 责任印制: 乔 宇

北京四季青印刷厂印刷

2009 年 5 月第 1 版第 1 次印刷

184mm×260mm·17 印张·420 千字

0001—3000 册

标准书号: ISBN 978-7-111-26698-3

定价: 39.00 元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换
销售服务热线电话: (010) 68326294

购书热线电话: (010) 88379639 88379641 88379643

编辑热线电话: (010) 88379764

封面防伪标均为盗版

西门子自动化产品培训用书

编 委 会

主 编	边春元	满永奎				
副主编	任双艳	王志强				
编 委	姜雪松	李艳杰	李爱平	邓 伟	王 璐	
	崔广臣	刘长勇	孙亦红	李 策	孟晓芳	
	王 珏	于艳秋	王卫红	胡 博	田有文	
	王 俊	解东光	王宇龙	杨 晨	杨 萍	

丛 书 序

当今科技的飞速发展，对于改变人类社会的生产和生活面貌，推动人类社会的物质文明和精神文明向前发展，无疑具有极其重要的作用和意义。作为一门现代科学技术，自动化技术反映了人们改造大自然的能力，它是多种学科和技术的交叉与综合，尤其是在信息技术飞速发展和日益普及的今天，自动化新技术和新产品更是日新月异、层出不穷。毋庸置疑，自动化技术在推动社会进步、促进经济发展、改善生活质量和建设可持续发展的和谐社会等方面将发挥越来越重要的作用。

西门子（Siemens）公司是当今世界上最大的电气自动化公司之一，其自动化产品遍布于生产和生活的各个方面，电气自动化解决方案是其核心业务领域之一。以应用场合的可编程序控制器和各种控制系统配套解决方案为代表的西门子自动化产品，广泛应用于冶金、造纸、采矿、水处理、造船、石油和天然气、智能交通管理、工业服务和 IT 工厂解决方案等领域。

随着西门子自动化产品在我国各个应用领域的逐步普及和大量应用，需要掌握西门子自动化产品基础和实用开发技术的工程人员和技术人员等群体也在不断扩大，国内多所高等院校和高职高专院校也已先后开设了与西门子自动化产品相关的专业课程，要求某些专业的本科生和研究生必须学习这些课程。可见，西门子自动化产品开发技术已经成为广大院校师生、工程人员和技术人员等竞相掌握的一门重要技能。

随着西门子自动化产品的广泛应用，如何更好地使用西门子自动化产品？如何更好地在实践中进行西门子自动化产品的应用开发？如何更好地利用特定西门子自动化产品的内部资源来完成复杂项目的开发？……这些问题不断地在困扰着采用西门子自动化产品进行项目开发的相关人员。因此，如何帮助广大工程人员和技术人员迅速解决上述难题成为一个困扰已久的问题。目前，解决这个问题的重要手段就是在学习源头上多下功夫，即编写和出版一些高质量的科技图书。通过学习这些科技图书，读者能够解决在实际开发工作中遇到的各种困扰，真正地掌握西门子自动化产品的基础知识和各种实用开发技术，从而能够更快、更好地完成实际项目的开发。

通过多年的教学实践和培训经验以及广泛的技术交流，广大院校师生、工程人员和技术人员等需要全面系统地阐述西门子自动化产品的书籍，这些书籍不应以介绍产品手册内容为主，而是应该在介绍基础知识的基础上能够介绍具有实际工程背景的实例，同时能够对实际应用中的使用方法、开发技巧和涉及到的重要知识点进行重点阐述。

基于目前西门子自动化产品图书的现状，决定立项出版这套“西门子自动化产品培训用书”，以满足广大读者希望快速、全面地学习和掌握西门子自动化产品系列应用技术的迫切愿望。

这套丛书在总体上遵循循序渐进、理论与实践相结合的原则，内容涵盖了西门子 S7 系



列 PLC、变频器、现场总线、工业网络、触摸屏、STEP7、WinCC、PLC 的梯形图与语句表编程方法等内容。另外，编写本丛书的目的不仅是对所积累知识的一个总结，更希望能将它与广大读者分享，共同探讨与进步。概括起来，这套丛书的主要特点体现在以下方面：

内容全面、体系完备：从不同层面和深度介绍利用西门子自动化产品开发工具进行应用开发的全过程，内容翔实，覆盖面广。

实践性强、实例典型：最大程度地强调了实践性，书中所有的实例都经过验证可实现，并具有代表性，读者可通过实例对相应技术点有清晰直观的了解。

把握新知、结合实际：对西门子自动化系列产品的新知识、新特性作了详细的介绍。书中很多技术点都是作者已经在实际工作中大量运用的，它们是开发经验的提炼和总结，相信会给读者带来很大的帮助。

相信这套丛书对于读者掌握西门子自动化产品将发挥重要的作用，使读者能够对西门子自动化产品和技术有一个系统的、全面的、深入的理解，同时能够利用它们开发出满足需要的工业自动化控制系统。

最后对参与这套丛书编写工作的各位作者表示衷心的感谢，感谢大家为我国工业自动化的技术发展和人才培养所作的巨大努力！

同时，也恳切希望读者能够对这套丛书的不足之处提出宝贵意见和建议，以便再版时更正，从而更好地服务广大读者。

是为序。

本丛书编委会

前 言

随着信息技术与计算机技术的飞速发展，分布式控制系统在工厂自动化和过程自动化中的应用速度迅速增长，现场总线技术已成为工业网络通信中的佼佼者。信息技术的飞速发展，引起了自动化系统结构的变革，以网络为主干的自动化分布式控制系统成为行业发展的趋势。

工业网络知识已经成为当今自动化过程应用的重要内容，并深入到工业自动化的各个层次，从现场设备、可编程序控制器、I/O 设备到操作系统、驱动设备以及人机接口（HMI），网络的应用无处不在。而西门子公司的 S7-300/400 在大中型 PLC 中应用最广，市场占有率最高。为了让广大工业自动控制的技术人员快速掌握西门子 S7-300/400 工业网络通信技术，我们组织编写了本书。

本书共分 8 章。第 1 章介绍了工业网络的发展、特点、组成及简单工作原理；第 2 章介绍了 MPI 的网络结构、通信协议及网络组态实例；第 3 章介绍了工业以太网的特点、网络部件、交换机技术以及网络配置方案；第 4 章介绍了 PROFIBUS 的总线拓扑结构、通信协议、网络部件及网络组态；第 5 章介绍了 AS-i 的总线拓扑结构、网络部件、通信方式及传输机制；第 6 章介绍了点对点通信的硬件、通信协议及在用户程序中的实现；第 7 章介绍了 MODBUS 通信、PLC 与驱动装置的串行通信；第 8 章介绍网络路由的技术条件、组态编程器和 HMI 的网络路由功能。

本书的最大特点是理论结合实例，讲解系统易懂、内容翔实、方法简单实用，同时书中的内容通过实例讲解，让读者深入浅出地学习并达到举一反三的效果。书中的每个通信实例互为独立单元，图文并茂，条理清晰，深入浅出地阐述了通信协议的各个方面，便于初学者学习与使用。

本书既可作为高等院校工业自动化、电气工程、电工、机电一体化、计算机应用及相关专业高年级本科生和研究生可编程序控制器等课程的教材，同时也可以作为广大从事电气、电工行业的研发工程师、专业技术人员，以及正在学习 PLC 的专业人员的工具书或者培训教材。

全书由刘建昌、于洪磊、辛红和杜平等编写，书中包含了作者多年来从事教学工作或者项目设计开发工作的经验总结。在本书的编写过程中，沈阳工程学院的邓玮参加了第 2 章和第 5 章的编写工作，赵琰参加了第 7 章和第 8 章的编写工作，迟新利参加了第 4 章的编写工作，林盛对第 2~4 章的计算机设置进行了配图。另外，本书的编写还得到了东北大学电气自动化研究所的盛科、孙羽、傅振宇、孙艳、董晶晶、邢颖、朱莱、岳磊、于文刚的大力协助，这里对他们的辛勤劳动表示衷心的感谢！

由于现代科学技术发展迅速，工业网络的应用也日新月异，同时限于作者的理论水平和实际开发经验，加上时间仓促，书中难免有错漏或者不足之处，肯请广大读者和相关专家进行批评指正。

编 者

目 录

丛书序 前言

第 1 章 绪论 1

- 1.1 PLC 控制网络的基本特点和通信功能 1
- 1.2 数据通信 2
 - 1.2.1 数据传输方式的分类 2
 - 1.2.2 传输速率和线路通信方式 4
 - 1.2.3 差错控制方式和检错码 5
 - 1.2.4 传输介质 6
 - 1.2.5 串行通信接口标准 6
- 1.3 工业局域网概述 7
 - 1.3.1 计算机网络简介 7
 - 1.3.2 局域网的基础知识 8
 - 1.3.3 现场总线概述 12
- 1.4 S7-300/400 PLC 的通信网络概述 14
 - 1.4.1 工厂自动化系统网络 14
 - 1.4.2 S7-300/400 PLC 的通信网络 14

第 2 章 MPI 通信 17

- 2.1 MPI 概述 17
- 2.2 MPI 网络 17
 - 2.2.1 MPI 网络结构 17
 - 2.2.2 PLC-PLC、PLC-WinCC 之间的 MPI 通信方式 18
- 2.3 设置 MPI 参数 19
- 2.4 全局数据包通信实例 20
 - 2.4.1 全局数据包通信方式 20
 - 2.4.2 全局数据的结构 34
- 2.5 事件驱动的 GD 通信实例 36

- 2.6 无组态连接通信实例 37
 - 2.6.1 双边编程通信方式 37
 - 2.6.2 单边编程通信方式 39
- 2.7 组态连接通信实例 41
- 2.8 S7 PLC 与 WinCC 监控软件的 MPI 通信实例 48

第 3 章 工业以太网通信 53

- 3.1 工业以太网简介 53
 - 3.1.1 工业以太网的特点 53
 - 3.1.2 工业以太网的构成 53
 - 3.1.3 工业以太网的特性 54
 - 3.1.4 工业以太网的优势 54
 - 3.1.5 工业以太网技术的发展趋势与前景 55
- 3.2 工业以太网的网络部件 56
 - 3.2.1 S7-300/400 的工业以太网通信处理器 57
 - 3.2.2 PC/PG 的工业以太网通信处理器 58
- 3.3 工业以太网的交换机技术 58
- 3.4 自适应与冗余网络 59
- 3.5 工业以太网的网络方案 60
 - 3.5.1 工业以太网方案 60
 - 3.5.2 以太网和高速以太网的工业过程 60
- 3.6 S7-300/400 的以太网解决方案 61
 - 3.6.1 西门子公司支持的网络协议和服务 61
 - 3.6.2 基于以太网的 S7 通信 63
 - 3.6.3 基于以太网的 S5 兼容通信 68
 - 3.6.4 两套 S7-300 之间的以太网通信 71



- 3.6.5 S7-200 与 S7-300/400 的以太网通信实例 78
- 3.6.6 通过 S7-300/400 CPU 集成工业以太网接口以 OPEN IE 通信 102

第 4 章 PROFIBUS 通信 106

- 4.1 PROFIBUS 概述 106
- 4.2 PROFIBUS 总线拓扑结构 108
 - 4.2.1 PROFIBUS 传输技术 108
 - 4.2.2 光纤传输技术 112
- 4.3 PROFIBUS 的通信协议 112
 - 4.3.1 总线存取协议 112
 - 4.3.2 PROFIBUS 网络的配置方案 114
 - 4.3.3 PROFIBUS 的协议结构和类型 115
 - 4.3.4 PROFIBUS 总线和总线终端器 116
- 4.4 PROFIBUS 总线的设置和属性 117
- 4.5 PROFIBUS 的网络部件 121
 - 4.5.1 PROFIBUS 的通信处理器模块 121
 - 4.5.2 PROFIBUS 的其他网络部件 122
- 4.6 利用 STEP7 组态 PROFIBUS-DP 通信网络 123
 - 4.6.1 CPU 集成 PROFIBUS-DP 接口连接 ET 200M 远程站 124
 - 4.6.2 支持 PROFIBUS-DP 协议的第三方设备通信 130
 - 4.6.3 通过 PROFIBUS-DP 连接智能从站 134
 - 4.6.4 一主站多从站的 PROFIBUS-DP DX 通信 147
 - 4.6.5 多主站的 PROFIBUS-DP DX 通信 159
 - 4.6.6 S7-300 与 MM440 变频器的连接 168
- 4.7 系统功能和系统功能块在 PROFIBUS-DP 通信中的应用 176
 - 4.7.1 SFC14 和 SFC15 的应用 176
 - 4.7.2 CP 342-5 作从站与 FC1 (DP_SEND)、

FC2 (DP_RECV) 的应用 183

4.7.3 SFC7 “DP_PRAL” 的应用 189

第 5 章 AS-i 通信 192

- 5.1 AS-i 概述 192
- 5.2 AS-i 总线拓扑结构 193
 - 5.2.1 AS-i 总线拓扑类型 193
 - 5.2.2 AS-i 总线连接方式 195
- 5.3 AS-i 网络部件 195
 - 5.3.1 AS-i 主站模式 195
 - 5.3.2 AS-i 从站模式 196
- 5.4 AS-i 的工作模式 198
- 5.5 AS-i 的通信方式 199
 - 5.5.1 寻址模式 199
 - 5.5.2 AS-i 通信过程 199
- 5.6 AS-i 的传输机制 200
 - 5.6.1 信号调制过程 200
 - 5.6.2 数据解耦 201
 - 5.6.3 访问方式和报文结构 201
 - 5.6.4 传输故障特征 203
- 5.7 从站编址 203
 - 5.7.1 通过手持编址单元编址 203
 - 5.7.2 通过 AS-i 主站编址 204
- 5.8 AS-i 主站的操作模式 204

第 6 章 点对点通信 205

- 6.1 点对点通信的概述 205
- 6.2 点对点通信的硬件 205
 - 6.2.1 S7-300C 集成的 PtP 通信接口 205
 - 6.2.2 通信处理器 206
- 6.3 ASCII Driver 通信协议 206
 - 6.3.1 点对点通信协议概述 206
 - 6.3.2 ASCII Driver 通信协议应用 207
- 6.4 3964 (R) 通信协议 209
 - 6.4.1 3964 (R) 的控制字符与报文帧格式 209
 - 6.4.2 使用 3964 (R) 发送数据 210
 - 6.4.3 使用 3964 (R) 接收数据 211
- 6.5 RK-512 通信协议 212



6.5.1 RK-512 的报文帧	212
6.5.2 使用 RK-512 发送数据	212
6.5.3 使用 RK-512 读取数据	213
6.5.4 RK-512 通信协议的参数设置	214
6.6 NETR 和 NETW 编程指令	214
6.6.1 指令格式	214
6.6.2 NETR/NETW 指令要点	215
6.6.3 调用 NETR/NETW 指令	215
6.6.4 NETR/NETW Wizard——网络读写 指令向导	216
6.7 点对点通信在用户程序中的 实现	220
6.7.1 调用系统功能块概述	220
6.7.2 ASCII/3964 (R) 的通信功能	221
6.7.3 RK-512 的通信功能	223
6.7.4 用于 PtP 通信处理器的 功能块	228
6.7.5 利用系统功能块编程	235
6.7.6 PPI 通信实例	238

第 7 章 串行通信

7.1 MODBUS 通信	248
---------------------	-----

7.1.1 支持 MODBUS 的通信处理器	248
7.1.2 支持 MODBUS 通信协议的接口 类型	248
7.1.3 MODBUS 通信协议及参数 组态	248
7.2 PLC 与驱动装置串行通信	252
7.2.1 USS 通信功能块简介	252
7.2.2 驱动装置的 USS 端口配置	253
7.2.3 USS 通信的编程	255

第 8 章 网络路由功能

8.1 概述	257
8.2 网络路由的技术条件	258
8.3 组态编程器的网络路由功能	258
8.4 HMI 的网络路由功能	260
8.4.1 组态 S7 OPC Server 的网络路由 功能	260
8.4.2 上位机的网络路由功能	261
8.4.3 OP/TP 的网络路由功能	261

参考文献

第 1 章

绪 论

近些年来，随着计算机通信网络技术的日益成熟及企业对工业自动化程度要求的提高，自动控制系统也从传统的集中式控制向多元分布式控制发展。企业信息管理系统的覆盖范围也正逐渐地从传统的经营、管理信息扩展到工厂的主控信息及现场的控制信息，对于企业而言，需要将整个工厂的生产流程和自动化控制系统纳入到统一的信息管理平台中。

借助于强大的工业通信网络，企业的信息平台不仅可以对市场信息进行处理，还可以包括从原材料采购、生产加工到成品贮运的全部生产流程，这意味着，通过与工厂中强大的工业通信网络的集成，企业信息管理系统可以实现对生产、物流、销售和管理信息的统一集成处理，为企业信息管理控制一体化功能的实现提供了坚实的基础。强大的工业通信网络与信息技术的结合彻底改变了传统的信息管理方式，将企业的生产管理带到了一个全新的境界。

1.1 PLC 控制网络的基本特点和通信功能

随着生产技术的发展，必然会使 PLC 的应用从单机向全厂生产自动化过渡。这就要求 PLC 之间、PLC 与计算机和其他控制设备之间能迅速、准确、及时地进行通信，以便能步调一致地进行控制和管理。

1. PLC 控制网络的基本特点

PLC 是工业领域基础自动化的主要工具，其通信系统应具有各种不同的功能和性能，以满足点对点通信、组成 PLC 网络，完成上下级控制系统之间的数据交换等不同的要求。最严格的要求就是在工业应用环境中保证数据传输的可靠性。

为了满足自动化系统对 PLC 网络的要求，PLC 控制网络应具有以下特点：

(1) 传输介质和连接组件标准化 在一个网络控制的环境中，需要相互通信的自动化部件分布广泛，加入的点很多，因此传输介质和接口组件使用数量很大，这就要求传输介质和接口组件一方面使用量要少，另一方面要互相兼容。

(2) 传输高可靠性 PLC 控制网络用于工业环境中，如果在传输过程中出错的数据不能及时检测出来并加以纠正，将会给控制过程造成巨大的危害。

(3) 良好的系统扩展性 一个自动化系统的结构有可能要经常更改或变动，这时需要网络系统也要作相应的调整，这种变动应该简单易行并且对系统的影响尽可能小。



(4) 良好的覆盖面积 由于进行自动化控制的工厂和车间常常是相当分散的, PLC 控制网络必须具有足够的传输距离, 以保证能在许多站之间任意通信。

(5) 较高的数据传输速率 随着技术的不断进步, 在自动化系统中, 需要处理和传输的数据量不断增加, 特别是当几个站同时要求通信时, 传输介质负荷非常大, 只有具备足够高的数据传输速率, 才能保证参加通信的每个站都能畅通地与其他站通信, 获得最短的响应时间。

2. PLC 的通信功能

PLC 通信功能有 3 种类型, 具体如下:

(1) 远程控制 远程控制属于 PLC 控制系统的扩展部分, PLC 进行远程的 I/O 控制, 它采用串行数据传输的方式将主站 PLC 与远处从站的 I/O 终端或 PLC 连接起来, 这时在主站一端应安装一个远程 I/O 主单元, 而在从站一端则要安装远程 I/O 从单元或称为 I/O 连接单元。

(2) PLC 局域网络系统 它是将分布在不同位置的 PLC 及其他数据终端设备 (DTE) 通过传输介质连接起来, 按照网络协议进行通信的系统。

(3) PLC 与上位机进行点对点通信 一台上位机可以连接多台 PLC, 这时各个 PLC 均可以接受上位机的命令, 并将执行结果送给上位机。这就构成了一个简单的“集中监督管理, 分散控制”的分布式控制系统。

1.2 数据通信

无论是计算机还是 PLC, 它们都是数字设备, 它们之间交换的信息是由“0”和“1”表示的数字信号。通常把具有一定的编码、格式和位长要求的数字信号称为数据信息。

数据通信就是将数据信息通过适当的传送线路从一台机器传送到另一台机器, 这里的机器可以是计算机、PLC 或是具有数据通信功能的其他数字设备。

数据通信系统的任务是把地理位置不同的计算机和 PLC 及其他数字设备连接起来, 高效率地完成数据的传送、信息交换和通信处理三项任务。数据通信系统一般由传送设备、传送控制设备和传送协议及通信软件等组成。

1.2.1 数据传输方式的分类

1. 串行传输与并行传输

按照传输数据的时空顺序分类, 数据通信的传输方式可以分为串行传输和并行传输两种。

(1) 串行传输 数据在一个信道上按位顺序传输的方式称为串行传输。其特点是串行传输通常只需要一或两根传输线, 在远距离传输时, 通信线路简单, 成本低; 但与并行传输相比, 传输速度慢, 故常用于传输距离远而对速度要求不高的场合。

(2) 并行传输 数据在多个信道同时传输的方式称为并行传输。其特点是传输速度快, 但由于一个并行数据有多少位二进制数, 就需要有多少根传输线, 因而成本高。通常, 并行传输用于传输速率高的近距离传输。



2. 频带传输与基带传输

数据传输系统根据在传输时由终端形成的数据信号是否进行了频谱搬移和是否进行了调制,可分为频带传输和基带传输两种。

(1) 频带传输 频带传输是把信号调制到某一频带上的传输方式。当进行频带传输时,用调制器把二进制信号调制成能在公共电话线上传输的音频信号(模拟信号)在通信线路上进行传输。信号传输到接收端后,再经过解调器的解调,把音频信号还原为二进制信号。这种以调制信号进行数据传输的方式称为频带传输,可采用3种方式进行调制:调幅、调频和调相。

1) 调幅是指根据数字信号的变化改变载波信号的幅度。例如传送“1”时为载波信号,传送“0”时为0,载波信号的频率和相位均未改变。

2) 调频是指根据数字信号的变化改变载波信号的频率。“1”时频率高,“0”时频率低,载波信号的幅度和相位均未改变。

3) 调相是指根据数字信号的变化改变载波信号的相位。数字信号从“0”变为“1”时或是从“1”变为“0”时载波信号的相位改变 180° ,但频率和幅度均未改变。

(2) 基带传输 基带是指电信号的基本频带。计算机、PLC及其他数字设备产生的“0”和“1”的电信号脉冲序列就是基带信号。基带传输是指数据传输系统对信号不做任何调制,直接传输数据的传输方式。

在PLC网络中,大多是采用基带传输,但是当传输距离较远时,则可以考虑采用调制解调器进行频带传输。为了满足基带传输的实际需要,通常要求把单极性脉冲序列经过适当的基带编码,以保证传输码型中不含有直流分量,并具有一定的检测错误信号状态的能力。

基带传输的传输码型很多,通常有曼彻斯特码(又称双相码)、差分双相码、密勒码、传号交替反转码和三阶高密度双极性码等。

在PLC网络中,采用较多的是曼彻斯特码的方式。主要原因是这种编码方式在传输过程中,为了避免当存在多个连续的“0”和“1”时系统无同步参考,故在编码中发送“1”时前半周期为低电平后半周期为高电平,传输“0”时前半周期为高电平后半周期为低电平。这样在每个码元的中心位置都存在着电平跳变,具有“内含时钟”的性质,即使连续传输多个“0”或“1”时,波形也有跳变,有利于提取定时同步信号。

基带传输方式使整个频带范围都用来传输某一数字信号(即单信道),常用于半双工通信。频带传输时,在同一传输线路上可用频带分割的方法将频带划分为几个信道,同时传输多路信号。例如传输两种信号,数据发送和传输使用高频信道,各站间的应答使用低频信道,常用于全双工通信。

3. 异步传输和同步传输

发送端和接收端之间的同步问题是数据通信中的重要问题。同步进行得不好,轻者导致误码增加,重者使整个系统不能正常工作。根据在串行通信中采用同步技术的不同,传输方式可分为异步传输和同步传输。

(1) 异步传输 异步传输也称为起止式传输,它是利用起止法来达到收发同步的。在异步传输中,被传输的数据编码为一串脉冲,每一个传输的字符都有一个附加的起始位和多个停止位。字节传输由起始位“0”开始,然后是被编码的字节。通常规定低位在前,高位



在后,接下来是校验位(可省略),最后是停止位“1”(可以是1位、1.5位或2位,用以表示字符的结束)。例如传输一个ASCII字符(7位),若选用2位停止位、1位校验位和1位起始位,那么传输这个7位ASCII字符需要11位。其格式如图1-1所示。



图 1-1 异步传输格式

(2) 同步传输 同步传输是把每个完整的数据块(帧)作为整体来传输,而不是按异步传输时每个字符都附加起始位和停止位的方式传输,因此在需要传输大量数据块的场合,用同步传输可以克服异步传输效率低的缺点。

为了使接收设备能够准确地接收数据块的消息,同步传输在数据开始处用同步字符“SYN”来指示,由定时信号(同步时钟)来实现发送端和接收端同步,一旦检测到与规定的字符相符合,接下去就是按顺序传输数据。但同步传输所需要的软件、硬件的价格比异步传输的高,因此常在数据传输速率较高的系统中才采用同步传输。同步传输格式如图1-2所示。

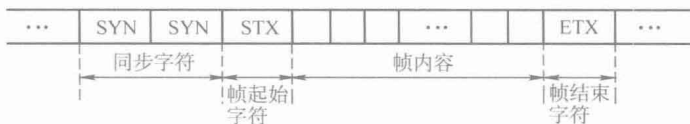


图 1-2 同步传输格式

1.2.2 传输速率和线路通信方式

1. 传输速率

传输速率是指单位时间内传输的信息量,它是衡量系统传输的主要指标。在数据传输中定义了3种速率:调制速率、数据信号速率和数据传输速率。

(1) 调制速率 调制速率也称码元速率,是脉冲信号在经过调制后的传输速率。即信号在调制过程中,单位时间内调制信号波形的变化次数,也就是单位时间内所能调制的调制次数,单位是波特,通常用于表示调制解调器之间传输信号的速率。

(2) 数据信号速率 数据信号速率是单位时间内通过信道的信息量,单位是比特/秒(bit/s)表示。调制速率和数据信号速率在串行传输二进制调制信号时,两者的速率在数值上是相同的。

通常,并不严格区分调制速率和数据信号速率,而是笼统地将它们称为传输速率(又称波特率),其单位是波特,即每秒传送是二进制位数,用bit/s表示。

(3) 数据传输速率 数据传输速率是指单位时间内传输的数据量,数据量的单位可以是比特、字符等,通常以字符/分钟为单位。例如使用数据信号速率为1800bit/s的传输电路,按异步传输方式来传输ASCII码数据时,其数据传输速率为

$$\text{数据传输速率} = (1800 \times 60) / (8 + 2) \text{ 字符/min} = 10800 \text{ 字符/min}$$

式中,分母中的“2”是指在一个字符位附加的起始位和终止位。

2. 线路通信方式

数据在通信线路上传输有方向性,按照数据在某一时间传输的方向,线路通信方式可分为单工通信、半双工通信和全双工通信方式。

(1) 单工通信方式 单工通信是指信息的传输始终保持同一方向,而不能进行反向传

输,如图 1-3 所示。其中甲站只能作为发送端,乙站只能作为接收端。

(2) 半双工通信方式 半双工通信是指信息流可以在两个方向上传输,但同一时刻只限于一个方向传输,如图 1-4 所示。其中甲站和乙站都具有发送和接收的功能,但传输线路只有一条,或者甲站发送乙站接收;或者乙站发送甲站接收。

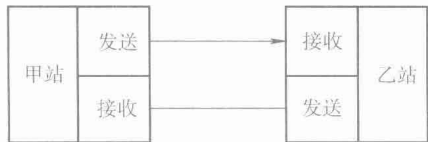


图 1-3 单工通信



图 1-4 半双工通信

(3) 全双工通信方式 全双工通信能在同一个方向上同时发送和接收,如图 1-5 所示。甲站和乙站双方都可以一面发送数据,一面接收数据。



图 1-5 全双工通信

1.2.3 差错控制方式和检错码

数据通信系统的基本任务是高效而无差错地传输和处理数据信息,数据通信系统的各个组成部分都存在着有差错的可能性。由于通信设备部分可以达到较高的可靠性,因此一般认为数据通信的差错主要来自于数据传输信道。数据信号经过远距离的传输,往往会受到各种的干扰,致使接收到的数据信号出现差错,引起数据信号序列的错误,在实际中,随机性的错误和突发性的错误通常是同时存在的。

1. 差错控制方式

差错控制是指对传输的数据信号进行检测错误和纠正错误。实际中常用的差错控制方式主要有以下 4 种:

(1) 自动检错重传 (ARQ) 在这种方式中,发送端按编码规则对拟发送的信号码附加冗余码后,再发送出去。接收端对收到的信号序列进行差错检测,判决有无错码,并通过反馈信道把判决结果送回到发送端。若判决有错码,发送端就重新发送原来的数据,直到接收端认为无差错为止;若判决为无错码,发送端就可以继续传送下一个新的数据。

(2) 前向纠错 (FEC) 在这种方式中,发送端按照一定的编码规则对拟发送的信号码元附加冗余码,构成纠错码。接收端将附加冗余码元按照一定的译码规则进行变换,检测信号中有无错码,若有错码,自动确定错码位置,并加以纠正。该方式物理实现简单,无需反馈信道,适用于实时通信系统,但译码器一般比较复杂。

(3) 混合纠错 混合纠错方式是前向纠错与自动检错重传两种方式的综合,发送端发送具有检测和纠错能力的码元,接收端将通过反馈信道要求发送端重新发送该信息。混合纠错方式综合了 ARQ 和 FEC 两者的优点,却未能克服它们各自的缺点,因而在实际应用中受到了一定的限制。

(4) 不用编码的差错控制 不用编码的差错控制是指不需要对传输的信号码元进行信号编码,而在传输方法中附加冗余措施来减少传输中的差错。



2. 检错码

常见的检错码有奇偶校验码和循环冗余校验（CRC）码等。由于奇偶校验码只需附加一位奇偶校验位进行编码，效率较高，因而得到了广泛的应用。

奇偶校验码是以字符为单位的校验方法。一个字符一般是由8位组成，低7位是信息字符的ASCII，最高位是奇偶校验位，该位可以是“0”也可以是“1”。其原则是：使整个编码中“1”的个数为奇数或偶数，若“1”的个数为奇数就称为奇校验，若“1”的个数为偶数就称为偶校验。

奇偶校验的原理是：若采用奇校验，发送端发送一个字符码（含有校验码），则“1”的个数一定是奇数，在接收端对“1”的个数进行统计，如果统计的结果“1”的个数为偶数，那一定意味着在传输过程中发生了差错。显然，若发生了奇数个位差错，接收端都可以发现，但若发生了偶数个位差错，接收端将无法查出。

1.2.4 传输介质

目前，普遍使用的传输介质有同轴电缆、双绞线、光缆，其他介质如无线电、红外线、微波等在PLC控制网络中应用很少。其中双绞线（带屏蔽）成本低，安装简单；光缆尺寸小，重量轻，传输距离远，但成本高，安装维修需专用仪器。

1.2.5 串行通信接口标准

近年来，串行通信发展很快，传输速率已达1Gbit/s，故在分布式工业检测系统中普遍采用串行数据通信。串行通信的连接接口与连接电缆的相互兼容是通信得以保证的基本要求，目前应用最广泛的串行通信接口标准有RS-232C、RS-422A和RS-485等。

1. RS-232C 标准

RS-232C是1969年由美国电子工业协会（EIA）所公布的串行通信接口标准。“RS”是“推荐标准”一词的英文缩写，“232”是标识号，“C”表示此标准修改的次数。它既是一种协议标准，又是一种电气标准，它规定了终端和通信设备之间信息交换的方式和功能。PLC与上位计算机之间的通信就是通过RS-232C标准接口来实现的。

RS-232C一般使用9针或25针的D型连接器，工业控制中9针连接器用得较多。

当通信距离较近时，通信双方可以直接连接，最简单的情况在通信中不需要控制联络信号，只需要三根线（发送线、接收线、信号线），便可以实现全双工异步串行通信，如图1-6所示。

RS-232C采用负逻辑，规定逻辑“1”电平为 $-15 \sim -5\text{V}$ ，逻辑“0”电平为 $+5 \sim +15\text{V}$ 。这样在线路上传送的电平可高达 $\pm 12\text{V}$ ，较之小于 $+5\text{V}$ 的TTL电平来说有更强的抗干扰能力。RS-232C标准中规定最大传输距离为15m（实际上可达30m），最高传输速率为20kbit/s，只能进行一对一的通信。

RS-232C使用单端驱动、单端接收电路，如图1-7所示。它是一种共地的传输方式，容易受到公共地线的电位差和外部引入的干扰信号的影响。

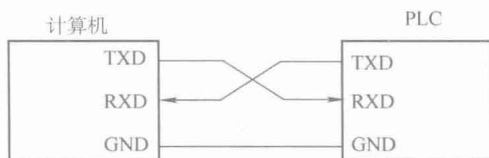


图 1-6 RS-232C 的信号线连接

2. RS-422A /485 标准

RS-422A 和 RS-485 接口标准均采用平衡驱动接收电路,如图 1-8 所示。其收发不共地,这可以大大减少共地所带来的共模干扰。



图 1-7 单端驱动单端接收

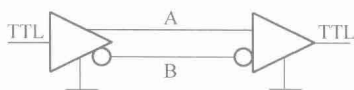


图 1-8 平衡驱动差分接收

RS-422A 与 RS-485 的区别是前者为全双工型,后者为半双工型。RS-422A 采用两对平衡差分信号线,如图 1-9 所示。

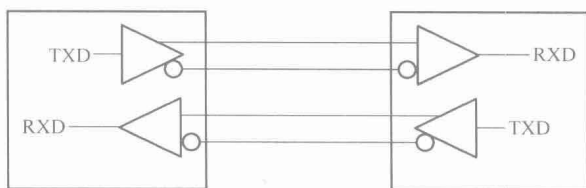


图 1-9 RS-422A 的点对点互连

RS-485 只需其中的一对,如图 1-10 所示。在 RS-485 互连中,某一时刻两个站中只有一个站可发送数据,而另一个站只能接收数据,因此,发送电路必须有使能端加以控制。

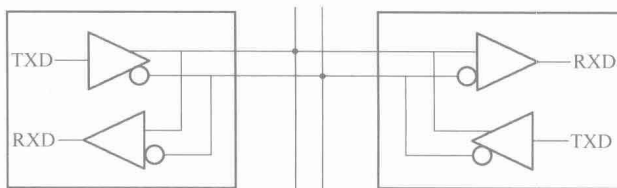


图 1-10 RS-485 的点对点互连

RS-422A/485 的驱动电路相当于两个单端驱动器,当输入统一信号时,使两个输出是反相的,差分接收器只接收差分输入电压,差分接收器可以区分 0.2V 以上的电位差,故即使存在共模干扰信号,也可进行长距离传输。

RS-422A/485 差分信号的传输线为双绞线,常用的双绞线的 Z_0 值为 100Ω ,因此两根信号线之间连接的匹配电阻值为 100Ω 。更为常用的端接方法是在每根信号线与地之间连接 50Ω 的电阻,这种方法有助于两根信号线保持平衡。

1.3 工业局域网概述

1.3.1 计算机网络简介

计算机网络是现在计算机技术与通信技术相结合的产物。它是指将地理位置不同且具有独立功能的多个计算机系统通过通信设备和线路将其连接起来,由功能完善的网络软件实现网络资源共享。计算机网络由计算机系统、通信链路和网络节点组成。

网络节点是双重作用的节点,用来负责管理和收发计算机系统的信息,通常是起着通信控制处理作用的接口装置。

通信链路是节点间的一条通信信道。为提高通信的可靠性,两节点之间可以采用一条以上的通信链路。

按所覆盖的地域范围大小,即通信距离远近划分,计算机网络可分为远程网、局域网和