

“十三五”江苏省高等学校重点教材（编号：2020-1-024）

“十二五”江苏省高等学校重点教材（编号：2013-1-027）

# 现场总线技术及其应用

第3版

主编 郭 琼 姚晓宁  
参编 刘志刚 单正娅 过志强  
主审 黄 麟



机械工业出版社

随着两化融合的深入发展,企业信息化建设需求明显,使得工业控制朝着智能化、网络化和集成化的方向发展。PLC 是设备控制、信息采集和数据通信的主要技术手段,是工业控制系统的核心,PLC 技术的相关课程则是高职自动化类专业的主干课程。本书以 PLC 通信为基础,详细介绍了 PROFIBUS、CC-Link、Modbus 以及工业以太网的技术特点、技术规范、系统设计、硬件组态及其在控制系统中的构建与应用。最后一章还介绍了现场总线系统集成概念、方法、原则,并通过对实际应用项目的分析阐述了现场总线技术应用的全过程。

本书在内容安排上强调现场总线技术的实际应用,紧密结合控制技术的新发展和新应用,实践教学内容丰富、结构合理,可作为高职高专院校自动化类专业的教材,也可作为从事现场总线系统设计与应用开发的技术人员的培训教材或参考资料。

本书配有微课视频,可扫描二维码观看。另外,本书配有电子课件,需要的教师可登录 [www.cmpedu.com](http://www.cmpedu.com) 免费注册,审核通过后下载,或联系编辑索取(微信:15910938545,电话:010-88379739)。

## 图书在版编目(CIP)数据

现场总线技术及其应用/郭琼,姚晓宁主编. —3 版. —北京:机械工业出版社,2021.4(2021.8 重印)

“十三五”江苏省高等学校重点教材

ISBN 978-7-111-66302-7

I. ①现… II. ①郭… ②姚… III. ①总线-技术-高等学校-教材  
IV. ①TP336

中国版本图书馆 CIP 数据核字(2020)第 144923 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:和庆娣 责任编辑:和庆娣 陈崇昱

责任校对:张艳霞 责任印制:李 昂

唐山三艺印务有限公司印刷

2021 年 8 月第 3 版·第 2 次印刷

184mm×260mm·14 印张·346 千字

标准书号:ISBN 978-7-111-66302-7

定价:59.00 元

电话服务

客服电话:010-88361066

010-88379833

010-68326294

封底无防伪标均为盗版

网络服务

机 工 官 网: [www.cmpbook.com](http://www.cmpbook.com)

机 工 官 博: [weibo.com/cmp1952](http://weibo.com/cmp1952)

金 书 网: [www.golden-book.com](http://www.golden-book.com)

机工教育服务网: [www.cmpedu.com](http://www.cmpedu.com)

# 前 言

现场总线由于满足工业控制系统向网络化、智能化、分散化发展的需求，得到了普遍关注和广泛应用，成为工业自动化技术发展的热点。特别是在我国智能制造背景下，其应用和进一步发展需求尤为突出。目前，生产系统的网络标准种类繁多，主要包括现场总线和工业以太网两大体系，仅在国际电工委员会的现场总线标准 IEC 61158 中，就有 20 种不同的现场总线技术标准，体现了工业领域多种总线并存、各自为战的局面。

目前，企业对现场总线及系统集成技术的人才需求迫切，这就要求高职高专院校积极培养熟悉现场总线及系统集成技术并能熟练使用该类技术的高技能应用型人才，从而满足企业转型升级、新技术新设备使用及生产组织方式和商业模式的创新与变革。现场总线及系统集成技术强调实际应用，在工业现场，其发展与相关的应用层出不穷。选取合适的教学内容和采用恰当的教学方法，是提高教学质量的关键。

本书在内容选取上遵循代表性、普遍性和发展性原则。

1) 西门子、三菱等品牌 PLC 在我国的应用较为普遍，也是高职相关课程中选用最多的 PLC 类型，不失一般性，在本书内容中以这两种主流 PLC 为学习载体，引进其相关的现场总线 PROFIBUS、CC-Link 作为学习内容。

2) Modbus 协议开放、应用广泛，常作为各种智能设备、智能仪表之间的通信标准，因此也将其通信内容作为教学的重点。

3) 以太网作为一项比较成熟的技术正向自动化领域逐步渗透，从企业决策层、生产管理调度层向现场控制层延伸并成为一种新的现场总线标准，将主流的 PROFINET、MC 协议 Modbus TCP 等技术纳入学习内容。

4) 在以上总线技术及载体的基础上，将主流集成技术融入系统开发、系统集成应用案例。

本书在编写时考虑到相关课程所涉及的知识点多、内容广以及高职高专学生的知识结构和定位，结合应用实际，以案例带动知识点开展学习，引导学生熟悉现场总线技术在分布式系统中的应用。

本书内容选择合理、层次分明、结构清楚、图文并茂、面向应用，适合作为高职高专院校电气自动化、工业过程自动化、机电一体化、工业机器人技术等专业的教学用书，也可作为工程人员的培训教材或相关科研人员的参考书。

本书由无锡职业技术学院郭琼、姚晓宁主编，无锡职业技术学院刘志刚、单正娅和无锡信捷电气股份有限公司过志强参编，无锡职业技术学院黄麟主审。

本书在编写过程中参考了大量书籍、文献、手册、会议资料及网络资源，在此向相关作者表示感谢。由于作者水平有限，且现场总线技术及应用一直在不断发展，本书中难免有不足之处，敬请读者批评指正。

编 者

## 二维码资源清单

| 序 号 | 资 源 名 称                               | 页 码 |
|-----|---------------------------------------|-----|
| 1   | 3-1 系统硬件组态                            | 59  |
| 2   | 3-2 主站程序编写                            | 62  |
| 3   | 3-3 系统调试与运行                           | 63  |
| 4   | 4-1 系统硬件配置与参数设置                       | 86  |
| 5   | 4-2 系统调试与运行                           | 91  |
| 6   | 5-1 系统硬件配置与参数设置                       | 121 |
| 7   | 5-2 FX <sub>3U</sub> 系列 PLC 通信参数及指令介绍 | 124 |
| 8   | 5-3 FX <sub>3U</sub> PLC 的程序编写        | 129 |
| 9   | 5-4 FX <sub>3U</sub> PLC 与智能仪表通信系统运行  | 131 |
| 10  | 6.3-1 300_300_PROFINET_硬件组态           | 140 |
| 11  | 6.3-2 300_300_PROFINET_程序编写           | 144 |
| 12  | 6.3-3 300_300_PROFINET_系统调试           | 145 |
| 13  | 6.5-1 系统硬件组态                          | 159 |
| 14  | 6.5-3 系统调试_功能码 01 读模式                 | 160 |
| 15  | 6.5-5 系统调试_功能码 01 写模式                 | 160 |
| 16  | 6.5-2 系统程序编写_功能码 01 读模式               | 160 |
| 17  | 6.5-4 系统现场运行_功能码 01 读模式               | 160 |
| 18  | 6.5-7 系统调试_功能码 03 使用                  | 161 |
| 19  | 6.5-6 系统程序编写_功能码 03 读和写模式             | 161 |

# 目 录

## 前言

## 二维码资源清单

|                       |    |
|-----------------------|----|
| 第 1 章 概述              | 1  |
| 1.1 控制系统的发展           | 1  |
| 1.2 现场总线及其发展          | 4  |
| 1.3 几种有影响力的现场总线       | 8  |
| 1.4 以太网与控制网络的结合       | 10 |
| 1.5 思考与练习             | 10 |
| 第 2 章 现场总线通信基础        | 12 |
| 2.1 现场总线的一些概念         | 12 |
| 2.1.1 基本术语            | 12 |
| 2.1.2 总线操作的基本内容       | 13 |
| 2.2 通信系统的组成           | 14 |
| 2.3 数据通信基础            | 15 |
| 2.3.1 数据通信的基本概念       | 15 |
| 2.3.2 数据编码            | 16 |
| 2.3.3 数据传输技术          | 17 |
| 2.3.4 网络拓扑结构与网络控制方法   | 22 |
| 2.3.5 数据交换技术          | 24 |
| 2.3.6 差错控制            | 25 |
| 2.4 通信模型              | 27 |
| 2.4.1 OSI 参考模型        | 27 |
| 2.4.2 现场总线通信模型        | 30 |
| 2.5 网络互联设备            | 31 |
| 2.6 现场总线控制网络          | 32 |
| 2.6.1 现场总线网络节点        | 32 |
| 2.6.2 现场总线控制网络的任务     | 33 |
| 2.6.3 控制网络的安全问题       | 33 |
| 2.7 思考与练习             | 34 |
| 第 3 章 PROFIBUS 总线及其应用 | 35 |
| 3.1 PROFIBUS 总线基础     | 35 |
| 3.1.1 PROFIBUS 总线及分类  | 35 |
| 3.1.2 PROFIBUS 的通信协议  | 36 |
| 3.2 PROFIBUS 的传输技术    | 40 |
| 3.2.1 RS-485 传输技术     | 40 |
| 3.2.2 光纤传输技术          | 43 |



|                                                          |            |
|----------------------------------------------------------|------------|
| 3.2.3 IEC 1158-2 传输技术 .....                              | 43         |
| 3.3 PROFIBUS-DP 控制系统 .....                               | 44         |
| 3.3.1 PROFIBUS-DP 设备 .....                               | 44         |
| 3.3.2 PROFIBUS-DP 的 IO 通信 .....                          | 45         |
| 3.3.3 GSD 文件 .....                                       | 46         |
| 3.4 基于智能从站 (PLC) 的 PROFIBUS-DP 通信实现 .....                | 47         |
| 3.4.1 控制系统硬件配置 .....                                     | 47         |
| 3.4.2 硬件组态 .....                                         | 48         |
| 3.4.3 通信接口参数设置 .....                                     | 52         |
| 3.4.4 程序设计与系统调试 .....                                    | 55         |
| 3.5 基于 DP 从站 (变频器) 的 PROFIBUS-DP 通信实现 .....              | 57         |
| 3.5.1 控制系统硬件介绍 .....                                     | 57         |
| 3.5.2 硬件组态及网络连接 .....                                    | 59         |
| 3.5.3 程序设计与系统调试 .....                                    | 62         |
| 3.6 实训项目 基于 S7-300 PLC 的现场总线系统构建与运行 .....                | 64         |
| 3.7 思考与练习 .....                                          | 65         |
| <b>第 4 章 CC-Link 总线及其应用 .....</b>                        | <b>66</b>  |
| 4.1 CC-Link 技术特点 .....                                   | 66         |
| 4.2 FX <sub>3U</sub> 系列 CC-Link 总线系统的构建 .....            | 68         |
| 4.2.1 系统网络配置 .....                                       | 68         |
| 4.2.2 主站模块 FX <sub>3U</sub> -16CCL-M .....               | 69         |
| 4.2.3 接口模块 FX <sub>3U</sub> -64CCL .....                 | 78         |
| 4.2.4 基于远程 I/O 站的 CC-Link 现场总线应用 .....                   | 85         |
| 4.3 Q 系列 CC-Link 总线系统的构建 .....                           | 94         |
| 4.3.1 Q 系列 PLC 介绍 .....                                  | 94         |
| 4.3.2 QJ61BT11 模块 .....                                  | 94         |
| 4.3.3 QJ61BT11 模块的应用 .....                               | 97         |
| 4.3.4 基于 Q 系列 PLC 的 CC-Link 现场总线应用 .....                 | 102        |
| 4.4 实训项目 CC-Link 总线控制系统的构建与运行 .....                      | 106        |
| 4.5 思考与练习 .....                                          | 107        |
| <b>第 5 章 Modbus 总线及其应用 .....</b>                         | <b>108</b> |
| 5.1 Modbus 协议 .....                                      | 108        |
| 5.2 Modbus RTU 通信 .....                                  | 109        |
| 5.3 实现 S7-200 PLC 之间的 Modbus RTU 通信 .....                | 111        |
| 5.3.1 Modbus 协议的安装 .....                                 | 111        |
| 5.3.2 Modbus 地址 .....                                    | 112        |
| 5.3.3 Modbus 通信的建立 .....                                 | 113        |
| 5.3.4 应用示例 .....                                         | 117        |
| 5.4 实现 FX <sub>3U</sub> PLC 与智能仪表之间的 Modbus RTU 通信 ..... | 121        |



|                                                               |            |
|---------------------------------------------------------------|------------|
| 5.4.1 控制要求及硬件配置 .....                                         | 121        |
| 5.4.2 智能仪表介绍 .....                                            | 122        |
| 5.4.3 FX <sub>3U</sub> 系列 PLC 通信参数及指令介绍 .....                 | 124        |
| 5.4.4 系统通信功能的实现 .....                                         | 129        |
| 5.5 实训项目 基于 PLC Modbus RTU 通信系统的构建与运行 .....                   | 132        |
| 5.6 思考与练习 .....                                               | 132        |
| <b>第 6 章 工业以太网及其应用</b> .....                                  | <b>133</b> |
| 6.1 工业以太网基础知识 .....                                           | 133        |
| 6.2 工业以太网的现状与发展前景 .....                                       | 136        |
| 6.2.1 工业以太网的现状 .....                                          | 136        |
| 6.2.2 工业以太网的发展前景 .....                                        | 136        |
| 6.3 PROFINET 技术及其应用 .....                                     | 137        |
| 6.3.1 PROFINET 技术介绍 .....                                     | 137        |
| 6.3.2 PROFINET 与 PROFIBUS 的比较 .....                           | 138        |
| 6.3.3 PROFINET IO 系统结构 .....                                  | 139        |
| 6.3.4 S7-300 PLC 与 S7-300 PLC 之间的 PROFINET 通信 .....           | 140        |
| 6.4 MC 技术及其应用 .....                                           | 147        |
| 6.4.1 MC 技术介绍 .....                                           | 147        |
| 6.4.2 FX <sub>3U</sub> PLC 与 SIMATIC HMI 的 MC TCP/IP 通信 ..... | 148        |
| 6.5 Modbus TCP 技术及其应用 .....                                   | 157        |
| 6.5.1 Modbus TCP 技术介绍 .....                                   | 157        |
| 6.5.2 S7-1200 PLC 之间的 Modbus TCP 通信功能的实现 .....                | 158        |
| 6.6 实训项目 基于 Modbus TCP 通信系统的构建与运行 .....                       | 166        |
| 6.7 思考与练习 .....                                               | 166        |
| <b>第 7 章 系统集成及应用</b> .....                                    | <b>167</b> |
| 7.1 系统集成内涵 .....                                              | 167        |
| 7.2 系统集成方法 .....                                              | 168        |
| 7.3 基于 Modbus RTU 的多站点互联通信系统 .....                            | 171        |
| 7.3.1 系统介绍 .....                                              | 171        |
| 7.3.2 硬件配置及通信参数设置 .....                                       | 171        |
| 7.3.3 S7-1200 PLC (主站) 程序设计 .....                             | 174        |
| 7.3.4 FX <sub>3U</sub> PLC (从站) 程序设计 .....                    | 176        |
| 7.3.5 系统调试 .....                                              | 177        |
| 7.4 基于组态软件的异构网络系统集成 .....                                     | 177        |
| 7.4.1 WinCC 软件介绍 .....                                        | 177        |
| 7.4.2 S7-200 PLC 与 S7-300 PLC 的系统集成 .....                     | 179        |
| 7.4.3 三菱 Q 系列 PLC 与 S7-300 PLC 的系统集成 .....                    | 184        |
| 7.5 基于 OPC 技术的异构网络系统集成 .....                                  | 188        |
| 7.5.1 KEPware 软件介绍 .....                                      | 188        |



|                                                         |     |
|---------------------------------------------------------|-----|
| 7.5.2 控制要求及硬件配置 .....                                   | 189 |
| 7.5.3 PLC 与 OPC 服务器的连接 .....                            | 189 |
| 7.5.4 S7-300 PLC 与 FX <sub>2N</sub> PLC 之间信息交互的实现 ..... | 193 |
| 7.6 基于工业网络的自动生产线控制系统集成 .....                            | 196 |
| 7.6.1 系统介绍 .....                                        | 196 |
| 7.6.2 系统硬件配置及组态 .....                                   | 197 |
| 7.6.3 RFID 信息识别功能的实现 .....                              | 199 |
| 7.6.4 MES 与 PLC 系统的集成 .....                             | 201 |
| 7.6.5 项目小结 .....                                        | 202 |
| 7.7 思考与练习 .....                                         | 202 |
| 附录 .....                                                | 203 |
| 附录 A TIA Portal V15 编程软件介绍 .....                        | 203 |
| A.1 TIA Portal 编程软件特点 .....                             | 203 |
| A.2 编程软件的安装 .....                                       | 204 |
| A.3 认识编程软件界面 .....                                      | 209 |
| 附录 B GX Developer 编程软件介绍 .....                          | 212 |
| B.1 编程软件及安装 .....                                       | 212 |
| B.2 创建工程 .....                                          | 212 |
| B.3 通信设置 .....                                          | 214 |
| 参考文献 .....                                              | 215 |

# 第 1 章 概 述

现场总线技术是一种用于工业生产现场，在现场设备之间、现场设备与控制装置之间实现双向、互连、串行、多节点的数字通信技术。现场总线控制系统的应用，大大降低了烦琐的布线工作量，且将控制功能下放到生产现场，使控制系统更为安全可靠、系统检测及控制单元分布更加合理，可实现工业现场的数据采集、自动控制和信息共享。

随着企业信息化的需求和智能制造建设的推进，以太网作为一项比较成熟的技术正向自动化领域逐步渗透，从企业决策层、生产管理调度层向现场控制层延伸。现场总线和工业以太网成为当前工业控制应用中普遍采用的技术，为企业实现远程监控、远程运维和管控一体化提供了基础。

## 学习目标

- ◇ 了解控制系统的发展过程。
- ◇ 掌握现场总线的概念、技术特点及发展趋势。
- ◇ 熟悉几种目前市场上有影响的现场总线名称及特点。
- ◇ 了解现场总线技术及工业以太网技术对未来自动控制系统的影响。

## 1.1 控制系统的发展

在工业和科学发展进程中，自动控制技术始终起着极为重要的作用，并广泛应用于各种领域，无论是在冶炼、化工、石油、电力，还是在造纸、纺织和食品等传统工业；无论是在航空、铁路等运输行业，还是在宇宙飞船、导弹制导等国防工业，抑或是在洗衣机、电冰箱等家用电器中，自动控制技术都得到了广泛的应用。

随着计算机技术、电子通信技术和控制技术的发展，工业控制领域已由单机控制逐步转变为网络化控制。计算机控制系统的结构从最初的直接式数字控制系统，到第二代的集散控制系统，发展到现在流行的现场总线控制系统。

### (1) 直接式数字控制系统

由于模拟信号精度低、信号传输的抗干扰能力较差，人们开始寻求用数字信号取代模拟信号，直接式数字控制便应运而生。直接式数字控制（Direct Digital Control, DDC）系统于 20 世纪七八十年代占主导地位。其采用单片机、微机或 PLC 作为控制器，控制器采用数字信号进行交换和传输，克服了模拟仪表控制系统中模拟信号精度低的缺陷，显著提高了系统的抗干扰能力。

图 1-1 为直接式数字控制系统示意图。计算机与生产过程之间的信息传递是通过生产过程的输入/输出设备进行的。过程输入设备包括输入通道（AI 通道、DI 通道），用于向计算机输入生产过程中的模拟信号、开关量信号或数字信号；过程输出设备包括输出通道

(AO 通道、DO 通道), 用于将计算机的运算结果输出并作用于控制对象。计算机通过过程输入通道对生产现场的变量进行巡回检测; 然后, 根据变量, 按照一定的控制规律进行运算; 最后, 将运算结果通过输出通道输出, 并作用于执行器, 使被控变量符合系统要求的性能指标。计算机控制系统由机箱、显示器、打印机、键盘及报警装置等设备组成, 可以实现对生产过程的自动控制、运行参数监视、打印运行参数数据及声光报警等功能。

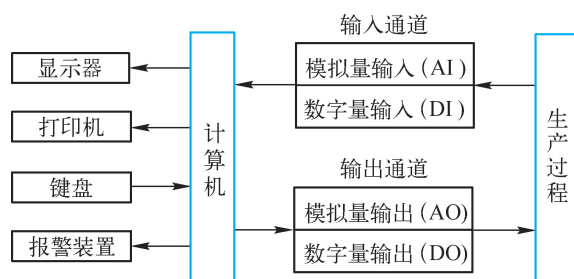


图 1-1 直接式数字控制系统示意图

DDC 系统属于计算机闭环控制系统, 它采用程序进行控制运算, 是计算机在工业生产中较为普遍的一种控制应用方式。这种控制方式灵活、经济, 只要改变控制算法和应用程序就可以实现对不同控制对象的控制甚至更为复杂的对象的控制, 系统可以满足较高的实时性和可靠性要求。但由于计算机直接承担 DDC 系统的控制任务, 一旦计算机出现故障, 就会造成该计算机所控制的所有回路瘫痪, 从而使控制系统的故障危险高度集中、运行风险增大。20 世纪 80 年代初, 随着计算机性能的提高和体积的缩小, 出现了内置 CPU 的数字控制仪表。基于“集中管理、分散控制”的理念, 在数字控制仪表以及计算机与网络技术的基础上, 人们又开发了集中与分散相结合的集散控制系统。

## (2) 集散控制系统

1975 年, 美国霍尼韦尔 (Honeywell) 公司首先推出世界上第一台集散控制系统 (Distributed Control System, DCS)——TDC2000 集散控制系统, 成为最早提出集散控制系统设计思想的开发商。此后, 国外的仪表公司纷纷研制出各自的集散控制系统, 应用较多的有美国福克斯波罗 (Foxboro) 公司的 SPECTRUM、美国贝利控制 (Bailey Controls) 公司的 Network90、英国肯特 (Kent) 公司的 P4000、德国西门子 (SIEMENS) 公司的 TELEPERM 以及日本横河 (YOKOGAWA) 公司的 CENTUM 等系统。我国使用 DCS 始于 20 世纪 80 年代初, 由吉化公司化肥厂在合成氨装置中引进了 YOKOGAWA 产品, 运行效果较好; 随后引进的 30 套大化肥项目和大型炼油项目都采用了 DCS 控制系统。同时, 坚持自主开发与引进技术相结合, 在 DCS 国产化产品开发方面取得了可喜的成绩, 比较有代表性的产品有浙江中控技术股份有限公司的 WebField ECS-700、北京和利时系统工程股份有限公司的 MACS 等系统。

集散控制系统于 20 世纪八九十年代占据主导地位, 它是一个由过程控制级和过程监控级组成的、以通信网络为纽带的多级计算机控制系统, 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, 下位机则分散下放到现场, 以实现分布式控制, 上/下位机通过控制网络互相连接以实现相互之间的信息传递。因此, 这种分布式的控制系统结构能有效地克服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, 并广泛应用于大型工业生产领域。

图 1-2 是一个典型集散控制系统的结构示意图，系统包括分散过程控制级、集中操作监控级和综合信息管理级，各级之间通过网络互相连接。分散过程控制级主要由 PLC、智能调节器、现场控制站及其他测控装置组成，是系统控制功能的主要实施部分；分散过程控制级直接面向工业对象，完成生产过程的数据采集、闭环调节控制、顺序控制等功能；并可与上一级的集中操作监控级进行数据通信。通信网络是 DCS 的中枢，它将 DCS 的各部分连接起来构成一个整体，使整个系统协调一致地工作，从而实现数据和信息资源的共享，是实现集中管理、分散控制的关键。集中操作监控级包括：操作员站、工程师站和层间网络连接器等，可实现系统操作、组态、工艺流程图显示以及监视过程对象和控制装置运行情况的功能，并可通过通信网络向过程控制级设备发出控制和干预指令。综合信息管理级由管理计算机构成，主要是指工厂管理信息系统，作为 DCS 更高层次的应用，它可以实现监视企业各部门的运行情况、完成生产管理和经营管理等功能。

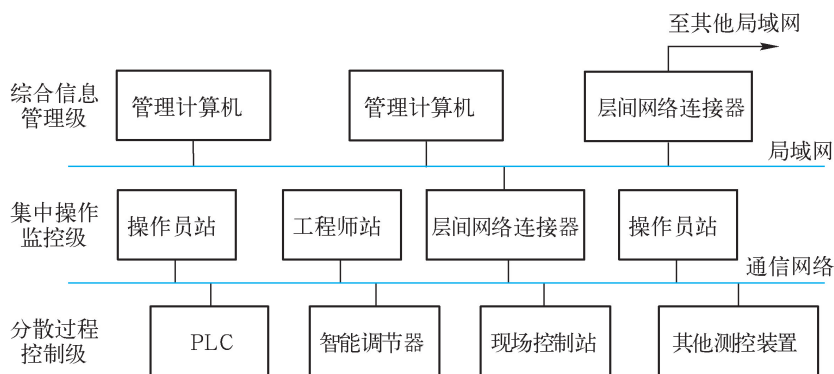


图 1-2 DCS 结构示意图

在集散控制系统中，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。但由于 DCS 系统在形成过程中，受计算机系统早期存在的系统封闭这一缺陷及厂家为达到垄断经营的目的对其控制通信网络采用封闭形式的影响，使得各厂家的产品自成系统，不同厂家的设备不能互连在一起，难以实现设备的互换与互操作，DCS 与上层 Intranet 和 Internet 信息网络之间实现网络互连和信息共享也存在很多困难，因此集散控制系统实质上是一种封闭专用的、不具备互操作性的分布式控制系统，而且系统造价昂贵。在这种情况下，用户对网络控制系统提出了开放性和降低成本的迫切要求。

为了降低系统的成本和复杂性，更为了满足广大用户对系统开放性、互操作性的要求，实现控制系统的网络化，现场总线迅速发展起来。

### (3) 现场总线控制系统

现场总线控制系统（Fieldbus Control System, FCS）是一种分布式控制系统，是在 DCS 的基础上发展起来的，它把 DCS 系统中由专用网络组成的封闭系统变成通信协议公开的开放系统，即可以把来自不同厂家而遵守同一协议规范的各种自动化设备，通过现场总线网络连接成系统，从而实现自动化系统的各种功能；同时，还将控制站的部分控制功能下放到生产现场，依靠现场智能设备本身来实现基本控制功能，使控制站可以集中处理更复杂的控制运算，更好地体现“功能分散、危险分散、信息集中”的思想。

现场总线技术产生于 20 世纪 80 年代，用于过程自动化、制造自动化、楼宇自动化等领

域的现场智能设备互连通信网络。按照国际电工委员会（International Electrotechnical Commission, IEC）对现场总线（Fieldbus）的定义：现场总线是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。它综合运用了微处理技术、网络技术、通信技术和自动控制技术，把通用或者专用的微处理器置入传统的测量控制仪表，使之具有数字计算和数字通信的能力；采用诸如双绞线、同轴电缆、光缆、微波、红外线和电力线等传输介质作为通信总线；按照公开、规范的通信协议，在位于现场的多个设备之间以及现场设备与远程监控计算机之间，实现数据传输和信息交换，形成各种适应实际需要的自动化控制系统。

现场总线控制系统的结构示意图如图 1-3 所示。现场总线作为智能设备的纽带，将挂接在总线上、作为网络节点的智能设备相互连接，构成相互沟通信息、共同完成自动控制功能的网络系统与控制系统。生产现场控制设备之间、控制设备与控制管理层网络之间通过这样结构的连接和通信，系统更加灵活和开放，为彻底打破自动化系统的信息孤岛创造了条件，使得设备之间以及系统与外界之间的信息交换得以实现，促进了自动控制系统朝着网络化、智能化的方向发展。它给自动化领域带来的变化，如同计算机网络给计算机的功能、作用带来的变化一样。如果说计算机网络把人类引入到信息时代，那么现场总线则使自控系统与设备加入到信息网络的行列，成为企业信息网络的底层，使企业信息沟通的范围一直延伸到生产现场。因此，可以说现场总线技术的出现标志着一个自动化新时代的开端。

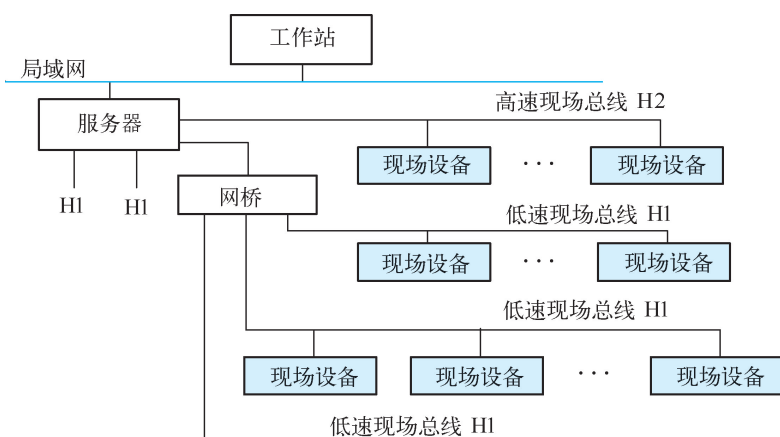


图 1-3 现场总线控制系统的结构示意图

## 1.2 现场总线及其发展

### 1. 现场总线的技术特点

根据国际电工委员会标准和现场总线基金会的定义，现场总线技术特点主要体现在以下几个方面。

#### (1) 现场设备互连

现场设备是指在生产现场安装的自动化仪器仪表，按功能可分为变送器、执行器、服务器和网桥等，这些现场设备通过双绞线、同轴电缆、光缆、红外线、微波等传输介质进行相互连接、相互交换信息。



## (2) 现场通信网络

现场总线作为一种数字式通信网络一直延伸到生产现场中的现场设备，使得现场设备之间互连、现场设备与外界网络互连，从而构成企业信息网络，完成生产现场到控制层和管理层之间的信息传递。

## (3) 互操作性

现场设备种类繁多，这就要求不同厂家的产品能够实现交互操作与信息互换，避免因选择了某一品牌的产品而被限制选择可使用设备的范围。用户把不同制造商的各种智能设备集成在一起，进行统一组态和管理，构成需要的控制回路。现场设备互连是最基本的要求，但只有实现设备的互操作性，才能使得用户能够根据需求自由集成现场总线控制系统。

## (4) 分散功能块

FCS 系统对 DCS 系统的结构进行了调整，摒弃了 DCS 的输入/输出单元和控制站，把 DCS 控制站的功能分散到现场具有智能的芯片或功能块中，使控制功能彻底分散，直接面对对象。如图 1-4 所示，压差变送器用来测量模拟输入量；而处理后的模拟输出量则用来控制调节阀；功能块 AI100 被置入变送器中，功能块 PID100、AO100 被置入调节阀中。由系统对这 3 个标准的功能块及其信号连接关系进行组态，并通过通信调度来执行控制系统的应用功能；将 AI 功能块的输出发送给 PID 功能块，把经过 PID 功能块运算得到的输出发送给 AO 功能块，由 AO 功能块的输出来控制阀门的开度，从而实现对被控流量的控制。

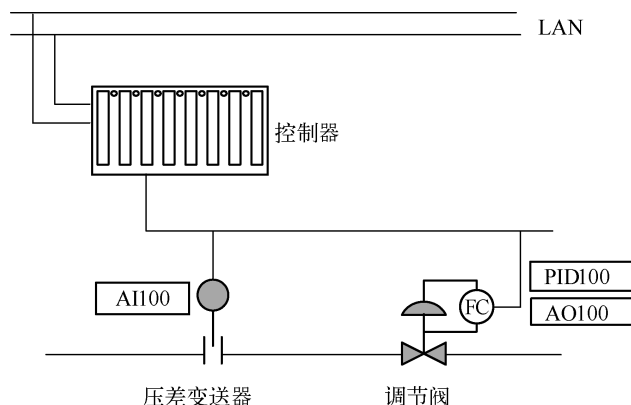


图 1-4 现场总线的分散功能块

由于将控制功能分散到多台现场仪表中，并可统一组态，所以用户可灵活选用各种功能块，构成所需的控制系统，彻底实现系统的分散控制。

## (5) 总线供电

总线在传输信息的同时，还可以给现场设备提供工作电源。这种供电方式能用于要求本质安全（简称为本安）环境的低功耗现场仪表，为现场总线控制系统在易燃易爆环境中的应用奠定了基础。

本质安全技术是在易燃易爆工作环境下使用电器设备时确保安全的一种方法。通常许多生产现场都有易燃易爆物质，为了确保设备及人身安全，必须采取安全措施，严格遵守安全防爆标准，以保证易燃易爆等工作场所的安全性。

本安电器设备与可燃性气体的接触将不会产生潜在的环境危险。整个系统的设计使得即



使在设备或连接电缆出现故障的情况下,可能出现的电火花或热效应也不足以引起燃烧或爆炸。本安技术仅适用于低电压和低功耗的设备。

#### (6) 开放式互联网络

现场总线为开放式互联网络,既可与同层网络互联,又可与不同层网络互联。其采用公开化、标准化、规范化的通信协议,只要符合现场总线协议,就可以把不同制造商的现场设备互连成系统,用户不需要在硬件或软件上花费太多精力,就可以实现网络数据库的共享。

通过以上阐述,现场总线控制系统(FCS)的关键要点如下:

- 1) FCS 的核心是现场总线,即总线标准。
- 2) FCS 的基础是数字智能现场装置。
- 3) FCS 的本质是信息处理现场化。

### 2. 现场总线的优越性

现场总线的优越性体现在以下几个方面。

#### (1) 开放性

现场总线的开放性主要包含两方面的含义。一方面其通信规约开放,也就是开发的开放性;另一方面能与不同的控制系统相连接,也就是应用的开放性。开放系统把系统集成的权利交给了用户,用户可按自己的需求,把来自不同供应商的产品组成大小随意、功能不同的系统。

#### (2) 互操作性和互用性

互操作性是指实现生产现场设备与设备之间、设备与系统之间信息的传送与沟通;而互用性则意味着不同生产厂家的同类设备可以进行相互替换从而实现设备的互用。

#### (3) 现场设备的智能化与功能自治性

现场总线将传感测量、补偿计算、工程量处理与控制等功能下放到现场设备中完成,因此单独的现场设备就可完成自动控制的基本功能,随时自我诊断运行状态。

#### (4) 系统结构的高度分散性

由于现场设备的智能化与功能自治性,使得现场总线构成了一种新型的全分布式控制系统的体系结构,各控制单元高度分散、自成体系,提高了系统的可靠性。

#### (5) 对现场环境的适应性

现场总线是专为工业现场设计的,可支持双绞线、同轴电缆、光缆、微波、红外线等传输介质,具有较强的抗干扰能力,可根据现场环境要求进行选择;能采用两线制实现通信与送电,可满足本质安全防爆要求。

由于现场总线本身所具有的技术特点,使得控制系统从设计、安装、投入运行到正常生产运行及检修维护等方面都体现出了极大的优越性。现场总线技术使自动控制设备与系统步入了信息网络的行列,为其应用开拓了更为广阔的领域。

### 3. 现场总线的标准

现场总线的发展是与微处理器技术、通信技术、网络技术等高新技术的发展及自动控制技术的不断进步分不开的。Honeywell 公司在 1983 年推出了 Smart 智能变送器,在原有模拟仪表的基础上增加了复杂的计算功能,并采用模拟信号与数字信号叠加的方法,使现场与控制室之间的连接由模拟信号过渡到数字信号,为现场总线仪表提出了新的发展方向。其后世界上各大公司相继推出了具有不同特色的智能仪表,如 Rosemount 公司推出了 1151 智能变



送器，Foxboro 公司推出了 820、860 智能变送器等，这些智能变送器带有微处理器和存储器，能够进行模拟信号到数字信号的转换处理，还可完成各种信号的滤波和预处理，给自动化仪表的发展带来了新的生机，为现场总线的产生奠定了一定基础。

国际电工委员会（IEC）非常重视现场总线标准的制定，早在 1984 年就成立了 IEC/TC65/SC65C/WG6 工作组起草现场总线技术标准（即 IEC 61158），但由于行业、应用地域的不同及产品推出的时间不同等多种因素，加上各公司和企业集团受自身利益的驱使，致使现场总线标准的制定工作进展十分缓慢，且形成了多种总线并存的局面，使得每种总线在应用与发展中都形成了自己的特点和应用领域。根据相关资料统计，已出现的现场总线有 100 多种，其中宣称为开放型总线的就有 40 多种。

现场总线的多样性使得它在短时间内难以统一，设备的互连、互通与互操作问题就很难解决，而以太网的优势可以使其延伸至过程控制领域，并已逐渐被工业自动化系统接受。为了满足实时性能应用的需要，各大公司和标准组织提出了各种提升工业以太网实时性的技术解决方案，产生了实时以太网（Real Time Ethernet，RTE）。

国际上对现场总线标准在不断地修订和增减，工作非常活跃。2007 年，第四版国际现场总线标准 IEC 61158 发布，具体类型见表 1-1 所示。其中，类型 6 Swift Net 总线因为市场推广应用不理想等原因被撤销。

表 1-1 IEC 61158（第四版）现场总线类型

| 类 型 | 名 称            | 类 型 | 名 称                      |
|-----|----------------|-----|--------------------------|
| 1   | TS 61158 现场总线  | 11  | TC-net 实时以太网             |
| 2   | CIP 现场总线       | 12  | EtherCAT 实时以太网           |
| 3   | PROFIBUS 现场总线  | 13  | Ethernet PowerLink 实时以太网 |
| 4   | P-Net 现场总线     | 14  | EPA 实时以太网                |
| 5   | FF HSE 高速以太网   | 15  | Modbus-RTPS 实时以太网        |
| 6   | Swift Net（已撤销） | 16  | SERCOSI, II 现场总线         |
| 7   | WorldFIP 现场总线  | 17  | VNET/IP 实时以太网            |
| 8   | Interbus 现场总线  | 18  | CC-Link 现场总线             |
| 9   | FF H1 现场总线     | 19  | SERCOSIII 实时以太网          |
| 10  | PROFINET 实时以太网 | 20  | HART 现场总线                |

IEC 61158 系列标准的各部分正陆续由全国工业过程测量控制和自动化技术委员会（SAC/TC124）转化为我国国家标准。

IEC 61158 系列标准代表了现场总线技术和实时以太网技术的最新发展。各主要企业在力推自己的总线产品的同时，也都尽力开发接口技术，将自己的总线产品与其他总线相连接。目前，现场总线技术还处于发展和完善阶段，标准的完善和统一在短期内还很难实现；总的来说，现场总线将向着工业以太网以及统一的国际标准方向发展。

#### 4. 对工业控制系统的影响

现场总线为工业控制系统向分散化、网络化、智能化发展提供了解决方法，它的出现使得目前生产的自动化仪表、集散控制系统、可编程序控制器在产品的体系结构、功能结构方面有了较大的变革，自动化设备的制造厂家被迫面临产品更新换代的又一次挑战。使得传统



的模拟仪表逐步向智能化数字仪表方向发展,并具有数字通信功能;出现了一批集检测、运算、控制功能于一体的变送控制器;出现了集检测温度、压力、流量于一体的多变量变送器;出现了带控制模块和具有故障诊断信息的执行器;并由此大大改变了现有的设备维护管理方法。因此,现场总线作为工业自动化技术的热点,受到了普遍的关注,且对企业的生产方式、管理模式都将产生深远的影响。

## 1.3 几种有影响力的现场总线

### 1. FF

FF 是基金会现场总线 (Foundation Fieldbus) 的简称,该总线是为了适应自动化系统,特别是过程自动化系统在功能、环境与技术上的需要而专门设计的。它得到了世界上主要的自动化系统集成商的广泛支持,在北美、亚太、欧洲等地区具有较强的影响力。

基金会现场总线采用国际标准化组织 (International Organization for Standardization, ISO) 的开放系统互连 (Open System Interconnection, OSI) 参考模型的简化模型,只具备了 OSI 参考模型 7 层中的 3 层,即物理层、数据链路层和应用层,另外增加了用户层。FF 分低速 H1 和高速 H2 两种通信速率, H1 用于过程自动化的低速总线,当其传输速率为 31.25 kbit/s 时,通信距离为 200~1900 m,可支持总线供电和本质安全防爆环境; H2 用于制造自动化的高速总线,当其传输速率为 1 Mbit/s 时,传输距离为 750 m,当其传输速率为 2.5 Mbit/s 时,传输距离为 500 m。随着现场总线和以太网的发展, H2 已经逐渐被高速以太网 (High Speed Ethernet, HSE) 取代,它满足了控制仪器仪表的终端用户对现场总线的互操作性、高速度、低成本等要求,充分利用低成本的以太网技术,并以 100 Mbit/s~1 Gbit/s 或更高的速度运行,主要应用于制造业的自动化以及逻辑控制、批处理和高级控制等场合。FF 的物理传输介质支持双绞线、光缆、同轴电缆和无线发射, H1 每段节点数最多 32 个, H2 每段节点数最多 124 个。

### 2. PROFIBUS

PROFIBUS 是 PROcess FieIdBUS 的缩略语,它是一种国际性的开放式现场总线标准,是由 SIEMENS 公司联合 E+H、Samson、Softing 等公司推出的,是符合德国标准 DIN 19245 和欧洲标准 EN 50170 的现场总线标准。

PROFIBUS 总线采用了 OSI 模型中的 3 层,即物理层、数据链路层和应用层,另外还增加了用户层,由 PROFIBUS-DP、PROFIBUS-FMS、PROFIBUS-PA 三个版本组成,可根据各自的特点用于不同的场合。DP 主要用于分散外设间的高速数据传输,适用于加工自动化领域; FMS 主要解决车间级通用性通信任务,完成中等速度的循环和非循环通信任务,适用于纺织、楼宇自动化等领域; PA 是专门为过程自动化设计的,可以通过总线供电、提供本质安全型,可用于危险防爆区域。PROFIBUS 采取主站之间的令牌传递方式和主、从站之间的主从通信方式。传输速率为 9.6 kbit/s~12 Mbit/s,最远传输距离可达到 1200 m,若采用中继器可延长至 10 km,传输介质为双绞线或者光缆,最多可挂接 127 个站点。

### 3. CAN

CAN 是控制器局域网 (Controller Area Network) 的简称,最早由德国 BOSCH 公司推出,



用于汽车内部测量与执行部件之间的数据通信，其总线规范已被国际标准化组织制定为国际标准，并得到了 Intel、Motorola、NEC 等公司的支持。

CAN 协议也是建立在国际化标准组织的开放系统互连模型基础上的，其模型结构为物理层、数据链路层及应用层 3 层；其信号传输介质为双绞线和光缆。CAN 的信号传输采用短帧结构，传输时间短；具有自动关闭功能，以切断该节点与总线的联系，使总线上的其他节点及其通信不受影响，具有较强的抗干扰能力。CAN 支持多主工作方式，并采用了非破坏性总线仲裁技术，通过设置优先级来避免冲突，传输速率最高可达 1 Mbit/s（传输距离为 40 m），传输距离最远可达 10 km（传输速率为 5 kbit/s），网络节点数实际可达 110 个。目前已有多家公司开发了符合 CAN 协议的通信芯片。

#### 4. Lonworks

Lonworks 是**局部操作网络**（Local Operating Networks）的缩略语，由美国 Echelon 公司于 1992 年推出，并由 Motorola、Toshiba 公司共同倡导。最初主要用于楼宇自动化，但很快发展到工业现场控制网。

Lonworks 采用 OSI 参考模型的全部 7 层通信协议，并采用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，其最高通信速率为 1.25 Mbit/s，传输距离不超过 130 m；最远通信距离为 2700 m，传输速率为 78 kbit/s，节点总数可达 32000 个。网络的传输介质可以是双绞线、同轴电缆、光纤、射频、红外线、电力线等多种通信介质，特别是电力线的使用，可将通信数据调制成载波信号或扩频信号，然后通过耦合器耦合到 220 V 或其他交直流电力线上，甚至是耦合到没有电力的双绞线上。电力线收发器提供了一种简单、有效的方法将神经元节点加入到电力线中，这样就可以利用已有的电力线进行数据通信，大大减少了通信中遇到的布线复杂等问题。这也是 Lonworks 技术在楼宇自动化中得到广泛应用的重要原因。

#### 5. CC-Link

CC-Link 是**控制与通信链路系统**（Control&Communication Link）的缩略语，1996 年 11 月由以三菱电机为主导的多家公司推出，目前在亚洲占有较大份额。在其系统中，可以将控制和信息数据同时以 10 Mbit/s 的高速传送至现场网络，在 10 Mbit/s 的传输速率下最远传输距离可以达到 100 m；而在 156 kbit/s 的传输速率下，最远传输距离可以达到 1200 m。如果使用电缆中继器和光中继器，则可以更加有效地扩展整个网络的传输距离。一般情况下，CC-Link 整个一层网络可由 1 个主站和 64 个子站组成，它采用总线方式通过屏蔽双绞线进行连接，广泛应用于半导体生产线、自动化生产线等领域。

作为开放式现场总线，CC-Link 是唯一起源于亚洲地区的总线系统，CC-Link 的技术特点尤其适合亚洲人的思维习惯。2005 年 7 月，CC-Link 被中国国家标准委员会批准为中国国家标准指导性技术文件。

#### 6. Modbus

Modbus 协议是**应用于电子控制器上的一种通用语言**，从功能上来看，可以认为它是一种现场总线。通过此协议，在控制器相互之间、控制器经由网络和其他设备之间都可以通信，它已经成为一种通用工业标准。

使用 Modbus 总线，不同厂商生产的控制设备可以连成工业网络，进行集中监控。此协议定义了一个控制器能识别使用的消息结构，而不管它们是经过何种网络进行通信的。



Modbus 的数据通信采用主从方式，主设备可以单独和从设备通信，也可以通过广播方式和所有从设备通信。Modbus 作为一种通用的现场总线，已经得到很广泛的应用，很多厂商的工控器、PLC、变频器、智能 I/O 与 A/D 模块等设备都具备 Modbus 通信接口。

## 1.4 以太网与控制网络的结合

控制网络的基本发展趋势是逐渐趋向于开放、透明的通信协议，而现场总线的开放性是有条件的、不彻底的，且多种总线并存已成定局，难以沿着开放的方向发展。当现场总线的发展遭遇到阻碍时，以太网技术作为一种解决方案得到迅猛的发展且被成功地用于工业控制网络，实现了办公自动化与工业自动化的无缝连接。

工业以太网是以太网技术在控制网络领域延伸的产物，是工业应用环境下信息网络与控制网络的完美结合。目前，对工业以太网没有严格的定义，各厂家推出的工业以太网在技术上也存在相当大的差距，比较典型的工业以太网技术有德国西门子公司主推的 PROFINET、法国施耐德电气公司主推的 Modbus TCP、德国倍福公司主推的 EtherCAT 等。一般来讲，工业以太网是指技术上与商用以太网（IEEE 802.3 标准）兼容，且在产品的设计时其材质的选用、产品的强度以及网络的实时性、可靠性、抗干扰性、安全性等方面能满足工业现场要求。工业以太网作为现场总线使用具有一定的优势，主要体现在以下几个方面。

1) **应用方便**：工业以太网是基于 TCP/IP 的以太网，它是一种标准的开放式通信网络，不同厂商的设备很容易互连。这种特性非常适合于解决控制系统中不同厂商设备的兼容和互操作等问题。

2) **价格低廉、组网容易**：由于信息网络的存在和以太网的大量使用，使得其具有价格明显低于控制网络相应软硬件的特点，如通过普通网卡就可将计算机连接到工业以太网网络中。

3) **技术支持广泛**：技术成熟、易于得到，已为许多人掌握，有利于企业网络的信息集成以及与上层网络的连接，便于实现企业管控一体化。

现场总线和工业以太网是当前工业控制应用中普遍采用的两种技术。工业以太网在一些行业的应用上已经真正实现了“一网到底”，但对于另一些行业，现场总线和工业以太网则在并存使用。现场总线存在着由于协议多、标准难以统一而导致的不同厂商设备之间的系统集成困难；而以太网在控制网络中存在的网络故障快速恢复、本质安全等问题则是制约其全面应用的主要障碍。

从目前国内外工业以太网技术的发展来看，工业以太网在控制层已得到广泛的应用。事实上，工业以太网已经成为一种新的现场总线标准。未来，工业以太网将在工业企业综合自动化系统现场设备之间的互连和信息集成中发挥越来越重要的作用。

## 1.5 思考与练习

1. 阐述 DDC 控制系统的结构及工作过程。
2. 什么是集散控制系统？其基本设计思想是什么？



3. 简述集散控制系统的层次结构及各层次所起的作用。
4. 什么是现场总线？现场总线技术特点体现在哪几个方面？
5. 现场总线的关键要点表现在哪几个方面？
6. 比较集散控制系统和现场总线控制系统的优缺点。
7. 常用的现场总线有哪些？它们各有什么特点？
8. 你认为现场总线对工业控制系统会产生怎样的影响？
9. 工业以太网作为现场总线具有哪些优势？
10. 谈谈你对现场总线的理解和看法。

## 第 2 章 现场总线通信基础

本章主要介绍现场总线通信系统的基本概念、数据通信的基础及其通信模型。现场总线控制网络是工业企业综合自动化的基础，用于完成数据采集、自动控制和信息共享等任务。现场总线控制网络可以通过网络互联技术实现不同网段之间的网络连接与数据交换，包括在不同传输介质、不同传输速率、不同通信协议的网络之间实现互联，从而更好地实现现场检测、采集、控制和执行以及信息的传输、交换、存储与利用的一体化，满足用户的需求。

由于现场总线通信的数据量较小，但对实时性、可靠性要求高，因此**现场总线通信模型**相对简单，简化了 OSI 参考模型，采用相应的补充方法实现被删除的 OSI 各层功能，并增设了用户层，具有结构简单、实时性好、通信速率快等优点。

### 学习目标

- ◇ 掌握数据通信及计算机网络的基本知识。
- ◇ 熟悉 OSI 分层通信模型的名称和功能。
- ◇ 了解数据封装和拆分的过程。
- ◇ 了解现场总线控制网络的特点和主要任务。

## 2.1 现场总线的一些概念

### 2.1.1 基本术语

#### 1. 总线与总线段

总线是多个系统功能部件之间传输信号或信息的公共路径，是遵循同一技术规范的连接与操作方式；使用统一的总线标准，不同设备之间的互连将更容易实现。一组设备通过总线相互连接在一起就称为总线段（Bus Segment）。总线段之间可以相互连接构成一个网络系统。

#### 2. 总线主设备与总线从设备

总线主设备（Bus Master）是指能够在总线上发起信息传输的设备，其具备在总线上主动发起通信的能力；总线从设备（Bus Slaver）是挂接在总线上、不能在总线上主动发起通信，只能对总线信息接收查询的设备。

总线上可以有多个设备，这些设备可以作为主站也可以作为从站；总线上也可以有多个主设备，这些主设备都具有主动发起信息传输的能力。但某一设备不能同时既作为主设备又作为从设备。被总线主设备连接上的从设备通常称为响应者，参与主设备发起的数据传送。

#### 3. 总线的控制信号

总线上的控制信号通常有 3 种类型，分别如下：



1) 控制设备的动作与状态。完成诸如设备清零、初始化、启动、停止等所规定的操作。

2) 改变总线操作方式。例如,改变数据流的方向、选择数据字段和字节等。

3) 表明地址和数据的含义。例如,对于地址,可以用于指定某一地址空间或表示出现了广播操作;对于数据,可以用于指定它能否转译成辅助地址或命令。

#### 4. 总线协议

总线协议 (Bus Protocol) 是管理主、从设备工作的一套规则,是事先规定的、共同遵守的规约。

#### 5. 控制网络

控制网络将多个分散在生产现场,且具有数字通信能力的测量、控制等设备作为网络节点,采用公开、规范的通信协议,以现场总线(包含工业以太网)作为通信连接的纽带,把现场控制设备连接成可以相互沟通信息,共同完成控制任务的网络系统。

### 2.1.2 总线操作的基本内容

#### 1. 总线操作

一次总线操作包括总线上的主设备与从设备之间建立连接、数据传送、接收、脱开等操作。所谓脱开 (Disconnected) 是指完成数据传送操作以后,主设备与从设备之间断开连接。主设备可以在执行完一次或多次总线操作后放弃总线占有权。

#### 2. 通信请求

通信请求是由总线上某一设备向另一设备发出传送数据或完成某种动作的请求信号,要求后者给予响应并进行某种服务。

总线的协议不同,通信请求的方式也就不同。最简单的方法是,要求通信的设备发出服务请求信号,相应的通信处理器检测到服务请求信号时就查询各个从设备,识别出是哪一个从设备要求中断并发出应答信号。该信号依次通过以菊花链方式连接的各个从设备,当请求通信的设备收到该应答信号时,就把自己的标识码放在总线上,同时该信号不再往后传递,这样通信处理设备就知道哪一个设备是服务请求者。这种传送中断信号的工作方式通常不够灵活,不适合总线上有多个进行通信处理设备的场合。

#### 3. 总线仲裁

系统中可能会出现多个设备同时申请对总线的使用权,为避免产生总线“冲突”(Contention),需要由总线仲裁机构合理地控制和管理系统中需要占用总线的申请者,在多个申请者同时提出使用总线请求时,以一定的优先算法仲裁哪个申请者应获得对总线的使用权。

总线仲裁用于裁决哪一个主设备是下一个占有总线的设备。某一时刻只允许某一个主设备占有总线,只有当它完成总线操作、释放总线占有权后,其他总线设备才允许使用总线。总线主设备为获得总线占有权而等待仲裁的时间叫作“访问等待时间”(Access Latency),主设备占有总线的时间叫作“总线占有期”(Bus Tenancy)。

总线仲裁操作和数据传送操作是完全分开且并行工作的,因此总线占有权的交接不会耽误总线操作。

#### 4. 寻址

寻址是主设备与从设备建立联系的一种总线操作,通常有物理寻址、逻辑寻址及广播寻



址3种方式。

1) 物理寻址用于选择某一总线段上某一特定位置的从设备作为响应者。由于大多数从设备都包含多个寄存器,因此物理寻址常常有辅助寻址,以选择响应者的特定寄存器或某一功能。

2) 逻辑寻址用于指定存储单元的某一个通用区,而不顾及这些存储单元在设备中的物理分布。某一设备监测到总线上的地址信号,看其是否与分配给它的逻辑地址相符,如果相符,它就成为响应者。物理寻址与逻辑寻址的区别在于前者是选择与位置有关的设备,后者是选择与位置无关的设备。

3) 广播寻址用于选择多个响应者。主设备把地址信息放在总线上,从设备将总线上的地址信息与其内部的有效地址进行比较,如果相符则该从设备被“连上”(Connect)。能使多个从设备连上的地址称为“广播地址”(Broadcast Addresses)。为了确保主设备所选择的全部从设备都能响应,系统需要有适应这种操作的定时机构。

每种寻址方式各有其特点和适用范围,逻辑寻址一般用于系统总线,物理寻址和广播寻址多用于现场总线。有的系统总线包含上述两种甚至3种寻址方式。

### 5. 数据传送

如果主设备与响应者连接上,就可以进行数据的读/写操作。读/写操作需要在主设备和响应者之间传递数据。“读”(Read)数据操作是读取来自响应者的数据;“写”(Write)数据操作是向响应者发送数据。为了提高数据传送的速度,总线系统可以采用块传送等方式,以加快长距离的数据传送速度。

### 6. 出错检测及容错

总线在传送信息时,有时会因传导干扰、辐射干扰等因素导致出现信息错误,使得“1”变成“0”,“0”变成“1”,影响到现场总线的性能,甚至于现场总线不能正常工作。除了要在系统的设计、安装、调试时采取必要的抗干扰措施以外,在高性能的总线中一般还设有出错码产生和校验机构,以实现传送过程的出错检测。例如,传送数据时如果有奇偶错误,通常是再发送一次信息。也有一些总线可以在保证很低的出错率的同时而不设检错机构。

为了减少设备在总线上因传送信息出错的故障对系统的影响,提高系统的重配置能力是十分重要的。例如,故障对分布式仲裁的影响要比菊花式仲裁小,菊花式仲裁在设备发生故障时会直接影响它后面设备的工作。现场总线系统能支持其软件利用一些新技术,实现如自动把故障隔离开来、实现动态重新分配地址、关闭或更换故障单元等功能。

### 7. 总线定时

主设备获得总线控制权以后,就进入总线操作,即进行主设备和响应者之间的信息交换,这种信息可以是地址也可以是数据。定时信号用于指明总线上的数据和地址何时有效。大多数总线标准都规定主设备可发起“控制”(Control)信号,如指定操作的类型、从设备状态响应信号等。

## 2.2 通信系统的组成

通信的目的是传送消息。实现消息传递所需的一切设备和传输介质的总和称为通信系

统，它一般由信息源、发送设备、传输介质、接收设备及信息接收者等几部分组成，如图 2-1 所示。

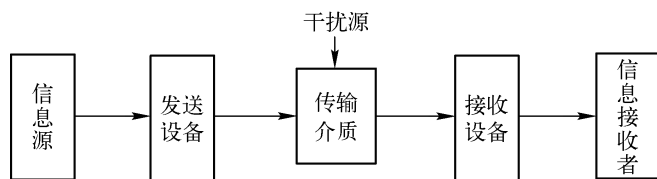


图 2-1 通信系统的组成

- 1) 信息源是产生消息的来源，其作用是把各种消息转换成原始电信号。
- 2) 信息接收者是信息的使用者，其作用是将复原的原始信号转换成相应的消息。
- 3) 发送设备的基本功能是将信息源产生的消息信号变换成适合在传输介质中传输的信号，使信息源和传输介质匹配起来。发送设备的变换方式是多种多样的，对数字通信系统而言，发送设备常常包括编码器与调制器。
- 4) 接收设备的基本功能是完成发送设备的反变换，即对信息进行解调、译码、解码等操作，它的任务是从带有干扰的接收信号中正确恢复出相应的原始基带信号，对于多路复用信号而言，还包括解除多路复用、实现正确分路等功能。
- 5) 传输介质是指发送设备与接收设备之间信号传递所经的媒介，它可以是电磁波、红外线等无线传输介质，也可以是双绞线、电缆、光缆等有线传输介质。
- 6) 干扰源是通信系统中各种设备以及信道中所固有的，并且是人们所不希望的。干扰的来源是多样的，可分为内部干扰和外部干扰；外部干扰往往是从传输介质引入的。在进行系统分析时，为了方便，通常把各种干扰源的集中表现统一考虑后再加入到传输介质中。

## 2.3 数据通信基础

### 2.3.1 数据通信的基本概念

所谓数据通信是指依据通信协议、利用数据传输技术在两个功能单元之间传递数据信息的技术，它可以实现计算机与计算机、计算机与终端、终端与终端之间的数据信息传递。

#### 1. 数据与信息

数据分为模拟数据和数字数据两种。模拟数据是指在时间和幅值上连续变化的数据，如由传感器接收到的温度、压力、流量、液位等信号；数字数据是指在时间上离散的、幅值经过量化的数据，它一般是由 0、1 的二进制代码组成的数字序列。

数据是信息的载体，它是信息的表示形式，可以是数字、字符、符号等。单独的数据并没有实际含义，但如果把数据按一定规则、形式组织起来，就可以传达某种意义，这种具有某种意义的数据集合就是信息，即信息是对数据的解释。

#### 2. 数据传输率

数据传输率是衡量通信系统有效性的指标之一，其含义为单位时间内传送的数据量，常用比特率  $S$  和波特率  $B$  来表示。

比特率  $S$  是一种数字信号的传输速率，表示单位时间（1 s）内所传送的二进制代码的

有效位 (bit) 数, 用每秒比特数 (bit/s)、每秒千比特数 (kbit/s) 或每秒兆比特数 (Mbit/s) 等单位来表示。

波特率  $B$  是一种调制速率, 指数据信号对载波的调制速率, 用单位时间内载波调制状态改变次数来表示, 单位为波特 (Baud)。或者说, 数据传输过程中线路上每秒钟传送的波形个数就是波特率  $B = 1/T$  (Baud)。

比特率和波特率的关系为

$$S = B \log_2 N$$

式中,  $N$  为一个载波调制信号表示的有效状态数; 如二相调制, 单个调制状态对应一个二进制位, 表示 0 或 1 两种状态; 四相调制, 单个调制状态对应两个二进制位, 有 4 种状态; 八相调制, 对应 3 个二进制位; 依此类推。

例如, 单比特信号的传输速率为 9600 bit/s, 则其波特率为 9600Baud, 它意味着每秒钟可传输 9600 个二进制脉冲; 如果信号由两个二进制位组成, 当传输速率为 9600 bit/s 时, 则其波特率为 4800Baud。

### 3. 误码率

误码率是衡量通信系统线路质量的一个重要参数; 误码率越低, 通信系统的可靠性就越高。它的定义为: 二进制符号在传输系统中被传错的概率, 近似等于被传错的二进制符号数与所传二进制符号总数的比值。

在计算机网络通信系统中, 误码率要求低于  $10^{-6}$ , 即平均每传输 1 Mbit 才允许错 1 bit 或更低。

### 4. 信道容量

信道是以传输介质为基础的信号通路, 是传输数据的物理基础。信道容量是指传输介质所能传输信息的最大能力, 以传输介质每秒钟能传送的信息比特数为单位, 常记为 bit/s, 它的大小由传输介质的带宽、可使用的时间、传输速率及传输介质质量等因素决定。

## 2.3.2 数据编码

计算机网络系统的通信任务是传送数据或数据化的信息, 这些数据通常以离散的二进制 0、1 序列的方式来表示。数字信号被传输时是以高电平或低电平的形式进行传输的, 所以需要将二进制数转换为高电平或低电平。数据编码技术就是研究在信号传输过程中如何进行编码。

计算机数据在传输过程中的数据编码类型, 主要取决于它采用的通信信道所支持的数据通信类型。根据数据通信类型, 网络中常用的通信信道分为两类: 模拟通信信道与数字通信信道。相应的用于数据通信的数据编码方式也分为两类: 模拟数据编码和数字数据编码。

模拟数据编码是用模拟信号的不同幅度、不同频率、不同相位来表达数据的 0、1 状态的; 而数字数据编码则是用高低电平的矩形脉冲信号来表达数据的 0、1 状态的。

采用数字数据编码方式时, 如果在基本不改变数据信号频率的情况下直接传输数字信号, 则称为基带传输方式。这是一种最为简单和经济的传输方式, 即在线路中直接传送数字信号的电脉冲, 不需要使用调制解调器, 就可以达到很高的数据传输速率和系统效率, 是目前应用较广的数据通信方式。

数字数据常采用不归零码、曼彻斯特编码和差分曼彻斯特编码等方式。

### 1. 不归零码

不归零 (Non-Return to Zero, NRZ) 码的波形如图 2-2a 所示, 用两种电平分别表示二进制信息 “1” 和 “0”, 这种编码方式信息密度高, 但不能提取同步信息且有误码积累。如果重复发送信息 “1”, 会出现连续发送正电流的现象; 如果重复发送信息 “0”, 会出现持续不送电流或持续发送负电流的现象, 使得信号中含有直流成分, 这是数据传输中不希望存在的分量。因此, NRZ 码虽然简单, 但只适用于极短距离传输, 在实际中应用并不多。

### 2. 曼彻斯特编码

曼彻斯特编码方式对每个码元都用两个连续且极性相反的脉冲表示, 其波形如图 2-2b 所示。每一位的中间都有一个跳变, 这个跳变既可作为时钟信号, 又可作为数据信号。其含义为: 从高到低的跳变表示 “1”, 从低到高的跳变表示 “0”。这种编码的特点是无直流分量, 且有较尖锐的频谱特性; 连续 “1” 或连续 “0” 信息仍能显示码元间隔, 有利于码同步的提取, 但带宽大。

### 3. 差分曼彻斯特编码

差分曼彻斯特编码利用码元开始处有无跳变来表示数据 “0” 和 “1”, 有跳变表示 “0”, 无跳变表示 “1”, 每位中间的跳变仅提供时钟定时, 其波形如图 2-2c 所示, 在每个比特周期中间产生跳变用以产生时钟, 这个跳变与数据无关, 只是为了方便同步。

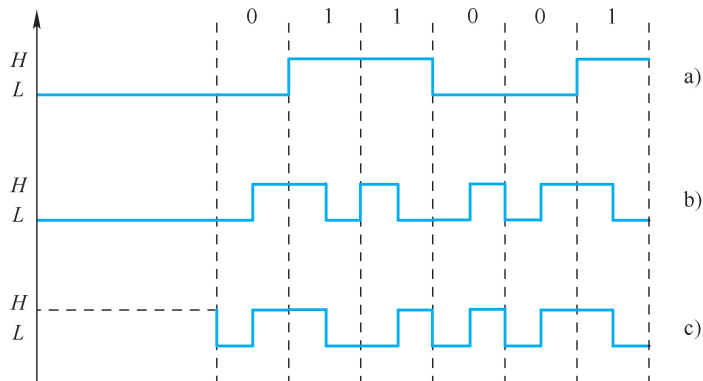


图 2-2 三种编码方式

a) 不归零码 (NRZ) 波形 b) 曼彻斯特编码波形 c) 差分曼彻斯特编码波形

曼彻斯特编码和差分曼彻斯特编码方法都是将时钟和数据包含在信号流中, 在传输代码信息的同时, 也将时钟同步信号一起传输到对方, 所以这种编码也称为自同步编码。

## 2.3.3 数据传输技术

数据传输方式可以分为串行传输和并行传输、单向传输和双向传输、异步传输和同步传输, 通过传输介质利用 RS-232C、RS-422A 及 RS-485 等通信接口标准进行信息交换。

### 1. 传输方式

#### (1) 串行传输和并行传输

1) 串行传输。串行通信时, 数据的各个不同位将分时使用同一条传输线, 从低位开始一位接一位按顺序传送, 数据有多少位就需要传送多少次, 如图 2-3 所示。串行通信多用于可程序控制器与计算机之间、多台可程序控制器之间的数据传送。串行通信虽然传输速率较慢, 但传输线少、连线简单, 特别适合多位数据的长距离通信。

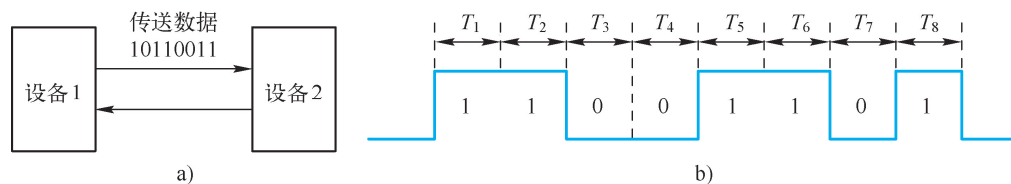


图 2-3 串行通信

a) 框图 b) 顺序传送

2) 并行传输。并行通信时，一个数据的所有位同时传送，因此每个数据位都需要一条单独的传输线，信息由多少个二进制位组成就需要多少条传输线，如图 2-4 所示。并行通信方式一般用于可编程序控制器内部的各元件之间、主机与扩展模块或近距离智能模块之间的数据处理。虽然并行传送数据的速度很快，传输效率高，但若数据位数较多、传送距离较远，则线路复杂、成本较高且干扰大，不适合远距离传送。

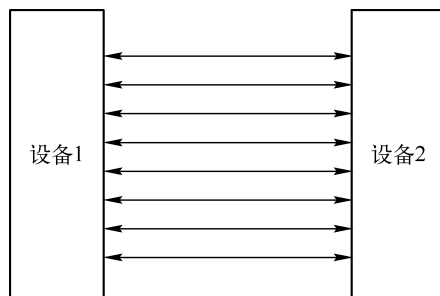


图 2-4 并行通信

## (2) 单向传输和双向传输

串行通信按信息在设备间的传送方向可分为单工、半双工和全双工 3 种方式，分别如图 2-5a、b、c 所示。

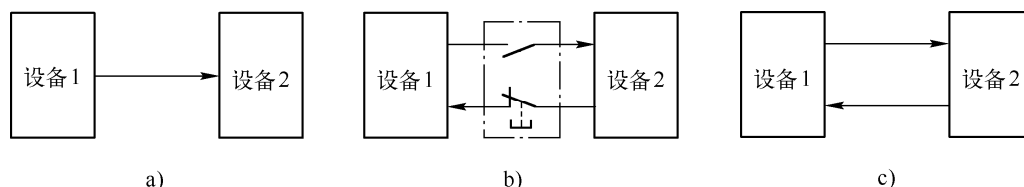


图 2-5 数据通信方式

a) 单工 b) 半双工 c) 全双工

单工通信是指信息的传递始终保持一个固定的方向，不能进行反方向传送，线路上任一时刻总是一个方向的数据在传送，例如无线广播；半双工是在两个通信设备中同一时刻只能有一个设备发送数据，而另一个设备接收数据，没有限制哪个设备处于发送或接收状态，但两个设备不能同时发送或接收信息，例如无线对讲机；全双工是指两个通信设备可以同时发送和接收信息，线路上任一时刻都可以有两个方向的数据在流动，例如电话。

## (3) 异步传输与同步传输

串行通信按时钟可分为异步传输和同步传输两种方式。

1) 在异步传输中，信息以字符为单位进行传输，每个信息字符都有自己的起始位和停止位，每个字符中的各个位是同步的，相邻两个字符传送数据之间停顿时间的长短是不确定



的，它是靠发送信息时同时发出字符的开始和结束标志信号来实现的，如图 2-6 所示。

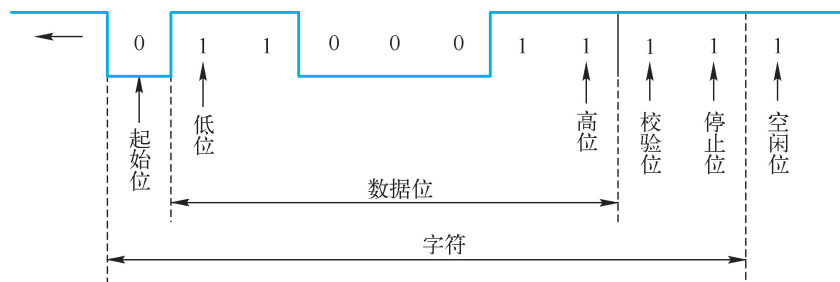


图 2-6 串行异步传送数据格式

2) 同步通信的数据传输是以数据块为单位的，字符与字符之间、字符内部的位与位之间都同步；每次传送 1~2 个同步字符、若干个数据字节和校验字符；同步字符起联络作用，用它来通知接收方开始接收数据。在同步通信中发送方和接收方要保持完全的同步，即发送方和接收方应使用同一时钟频率。

由于同步通信方式不需要在每个数据字符中加起始位、校验位和停止位，只需要在数据块之前加 1~2 个同步字符，所以传输效率高，但对硬件要求也相应提高，主要用于高速通信。采用异步通信方式传送数据时，每传一字节都要加入起始位、校验位和停止位，传送效率低，主要用于中、低速数据通信。

## 2. 接口标准

### (1) RS-232C 通信接口

串行通信时要求通信双方都采用标准接口，以便不同的设备方便地连接起来进行通信。RS-232C 接口（又称 EIA RS-232C）是目前计算机与计算机、计算机与 PLC 通信中常用的一种串行通信接口。

RS-232C 是美国电子工业协会（Electronic Industry Association, EIA）于 1969 年公布的标准化接口。“RS”是英文“推荐标准”（Recommand Standard）的缩写；“232”为标识号；“C”表示此接口标准的修改次数。它既是一种协议标准，又是一种电气标准，规定通信设备之间信息交换的方式与功能。

RS-232C 可使用 9 脚或 25 脚的 D 型连接器，如图 2-7 所示。这些接口线有时不会都用，简单的只需 3 条接口线，即“发送数据（TxD）、接收数据（RxD）和信号地（GND）”。常用的 RS-232C 接口引脚信号定义如表 2-1 所示。



图 2-7 D 型连接器



表 2-1 常用 RS-232C 接口引脚名称、功能及其引脚号

| 引脚名称 | 功能         | 25 脚连接器引脚号 | 9 脚连接器引脚号 |
|------|------------|------------|-----------|
| CD   | 载波检测       | 8          | 1         |
| RxD  | 接收数据       | 3          | 2         |
| TxD  | 发送数据       | 2          | 3         |
| DTR  | 数据终端设备准备就绪 | 20         | 4         |
| GND  | 信号公共参考地    | 7          | 5         |
| DSR  | 数据通信设备准备就绪 | 6          | 6         |
| RTS  | 请求传送       | 4          | 7         |
| CTS  | 清除传送       | 5          | 8         |
| RI   | 振铃指示       | 22         | 9         |

在电气特性上, RS-232C 中任何一条信号线的电压均为负逻辑关系: 逻辑“1”为  $-(5\sim 15)\text{V}$ ; 逻辑“0”为  $+(5\sim 15)\text{V}$ , 噪声容限为  $2\text{V}$ , 即接收器能识别高至  $+3\text{V}$  以上的信号作为逻辑“0”, 低到  $-3\text{V}$  以下的信号作为逻辑“1”。电气接口采用单端驱动、单端接收电路, 容易受到公共地线上的电位差和外部引入的干扰信号的影响。

RS-232C 只能进行一对一的通信, 其驱动器负载为  $3\sim 7\text{k}\Omega$ , 所以 RS-232C 适合本地设备之间的通信。传输率分为  $19200\text{ bit/s}$ 、 $9600\text{ bit/s}$ 、 $4800\text{ bit/s}$  等几种, 最高通信速率为  $20\text{ kbit/s}$ , 最远传输距离为  $15\text{ m}$ , 通信速率和传输距离有限。

### (2) RS-422A 通信接口

针对 RS-232C 的不足, EIA 又于 1977 年推出了串行通信接口 RS-499, 对 RS-232C 的电气特性进行了改进; RS-422A 是 RS-499 的子集, 它定义了 RS-232C 所没有的 10 种电路功能, 规定用 37 脚连接器。

在电气特性上, 由于 RS-422A 采用差动发送、差动接收的工作方式并使用  $+5\text{V}$  电源。因此, 在通信速率、通信距离、抗共模干扰等方面较 RS-232C 接口有较大的提高, 最大传输率可达  $10\text{ Mbit/s}$ , 传输距离为  $12\sim 1200\text{ m}$ 。

### (3) RS-485 通信接口

RS-485 是 RS-422A 的变形, RS-422A 是全双工通信, 两对平衡差分信号线分别用于发送和接收, 所以采用 RS-422A 接口通信时最少需要四根线。RS-485 为半双工通信, 只有一对平衡差分信号线, 不能同时发送和接收, 最少时只需两根连线。

在电气特性上, RS-485 的逻辑“1”以两线间的电压差  $+(2\sim 6)\text{V}$  表示, 逻辑“0”以两线间的电压差  $-(2\sim 6)\text{V}$  表示。接口信号电平比 RS-232C 低, 不易损坏接口电路的芯片。

由于 RS-485 接口能用最少的信号连线完成通信任务, 且具有良好的抗噪声干扰性、高传输速率 ( $10\text{ Mbit/s}$ )、长的传输距离 ( $1200\text{ m}$ ) 和多站功能 (最多 128 站) 等优点, 所以在工业控制中广泛应用, 例如西门子 S7 系列 PLC 采用的就是 RS-485 通信口。

## 3. 传输介质

传输介质也称传输媒质或通信介质, 是指通信双方用于彼此传输信息的物理通道。通常分为有线传输介质和无线传输介质两大类。有线传输介质使用物理导体提供从一个设备到另一个设备的通信通道; 无线传输介质不使用任何人为的物理连接, 通过空间来广播传输信

息。图 2-8 是传输介质的分类。在现场总线控制系统中常用的传输介质为双绞线、同轴电缆和光缆等，其外形结构分别如图 2-9a、b、c 所示。

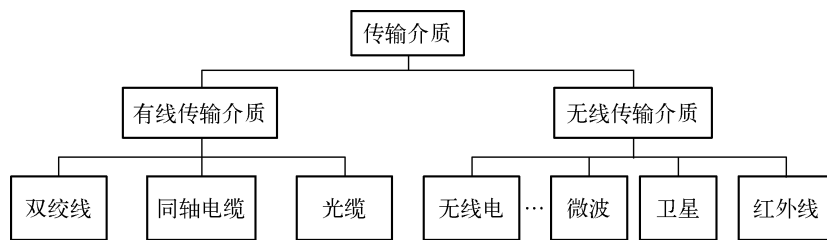


图 2-8 传输介质的分类

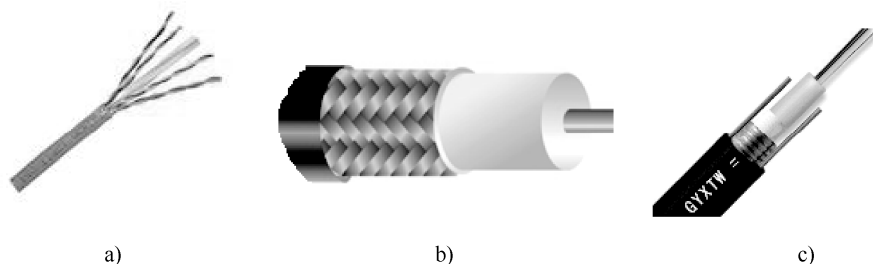


图 2-9 常用传输介质的结构

a) 双绞线 b) 同轴电缆 c) 光缆

### (1) 双绞线

双绞线是目前最常见的一种传输介质，用金属导体来接收和传输通信信号，可分为**非屏蔽双绞线**（Unshielded Twisted Pair, UTP）和**屏蔽双绞线**（Shielded Twisted Pair, STP）。

每一对双绞线由绞合在一起的相互绝缘的两根铜线组成。把两根绝缘的铜线按一定密度互相绞在一起，可降低信号干扰的程度，每一根导线在传输中辐射的电波也会被另一根导线上发出的电波抵消。如果把一对或多对双绞线放在一个绝缘套管中便成了双绞线电缆，如在局域网中常用的五类、六类、七类双绞线就是由 4 对双绞线组成的。

屏蔽双绞线由于有较好的屏蔽性能，所以也具有较好的电气性能。但由于屏蔽双绞线的价格较非屏蔽双绞线贵，且非屏蔽双绞线的性能对于普通的企业局域网来说影响不大，甚至说很难察觉，所以在企业局域网组建中所采用的通常是非屏蔽双绞线。

双绞线既可以传输模拟信号又可以传输数字信号，对于模拟信号，每 5~6 km 需要一个放大器；对于数字信号，每 2~3 km 需一个中继器。在使用时每条双绞线两端都需要安装 RJ-45 连接器才能与网卡、集线器或交换机相连接。

虽然双绞线与其他传输介质相比，在数据传输速率、传输距离和信道宽度等方面均受到一定的限制，但在一般快速以太网应用中影响不大，且价格较为低廉，所以目前双绞线仍是企业局域网中首选的传输介质。

### (2) 同轴电缆

如图 2-9b 所示，同轴电缆的结构分为 4 层。内导体是一根铜线，铜线外面包裹着泡沫绝缘层，再外面是由金属或者金属箔制成的导体层，最外面由一个塑料外套将电缆包裹起来。其中铜线用来传输电磁信号；网状金属屏蔽层一方面可以屏蔽噪声，另一方面可以作为信号地；绝缘层通常由陶制品或塑料制品组成，它将铜线与金属屏蔽层隔开；塑料外套可使



电缆免遭物理性破坏，通常由柔韧性好的防火塑料制品制成。这样的电缆结构既可以防止自身产生的电干扰，也可以防止外部干扰。

经常使用的同轴电缆有两种，一种是  $50\ \Omega$  电缆，用于数字传输，由于多用于基带传输，也叫基带同轴电缆；另一种是  $75\ \Omega$  电缆，多用于模拟信号传输。

常用同轴电缆连接器是卡销式连接器，将连接器插到插口内，再旋转半圈即可，因此安装十分方便。T 型连接器（细缆以太网使用）常用于分支的连接。同轴电缆的安装费用低于 STP 和五类 UTP，安装相对简单且不易损坏。

同轴电缆的数据传输速率、传输距离、可支持的节点数、抗干扰性能都优于双绞线，成本也高于双绞线，但低于光缆。

### （3）光缆

光导纤维是目前网络介质中最先进的技术，用于以极快的速度传输巨大信息的场合。它是一种传输光束的细微而柔韧的介质，简称为**光纤**。在它的中心部分包括了一根或多根玻璃纤维，通过从激光器或发光二极管发出的光波穿过中心纤维来进行数据传输。

光导纤维电缆由多束纤维组成，简称为**光缆**。光缆是数据传输中最有效的一种传输介质，它有以下几个特点。

1) 抗干扰性好。光缆中的信息是以光的形式传播的，由于光不受外界电磁干扰的影响，而且本身也不向外辐射信号，所以光缆具有良好的抗干扰性能，适用于长距离的信息传输以及安全要求较高的场合。

2) 具有更宽的带宽和更高的传输速率，且传输能力强。

3) 衰减少，无中继时传输距离远。这样可以减少整个通道的中继器数目，而同轴电缆和双绞线每隔几千米就需要接一个中继器。

4) 光缆本身费用昂贵，对芯材纯度要求高。

在使用光缆互连多个小型机的应用中，必须考虑光纤的单向特性，如果要进行双向通信，那么就应使用双股光纤，一个用于输入，一个用于输出。由于要对不同频率的光进行多路传输和多路选择，因此又出现了光学多路转换器。

光缆连接采用光缆连接器，安装要求严格，两根光缆间任意一段芯材未能与另一段光纤或光源对正，就会造成信号失真或反射，连接过分紧密则会造成光线改变发射角度的变化。

## 2.3.4 网络拓扑结构与网络控制方法

### 1. 网络拓扑结构

网络拓扑结构是指用传输介质将各种设备互连的物理布局。将在局域网（Local Area Network, LAN）中工作的各种设备互连在一起的方法有多种，目前大多数 LAN 使用的拓扑结构有**星形**、**环形**及**总线型**这 3 种网络拓扑结构。

星形结构如图 2-10a 所示，其连接特点是端用户之间的通信必须经过中心站，这样的连接便于系统集中控制、易于维护且网络扩展方便，但这种结构要求中心系统必须具有极高的可靠性，否则中心系统一旦损坏，整个系统便趋于瘫痪，对此中心系统通常采用双机热备份，以提高系统的可靠性。

环形结构在 LAN 中使用较多，如图 2-10b 所示，其连接特点是每个端用户都与两个相邻的端用户相连，直到将所有端用户连成环形。这样的点到点连接方式使得系统总是以单向

方式操作，如用户  $N$  是用户  $N+1$  的上游端用户，用户  $N+1$  是用户  $N$  的下游端用户，如果  $N+1$  端需要将数据发送到  $N$  端，则几乎要绕环一周才能到达  $N$  端。这种结构容易安装和重新配置，接入和断开一个节点只需改动两条连接，可以减少初期建网的投资费用；每个节点只有一个下游节点，不需要路由选择；可以消除端用户通信时对中心系统的依赖性，但某一节点一旦失效，整个系统就会瘫痪。

总线型拓扑结构在 LAN 中使用最普遍，如图 2-10c 所示，其连接特点是端用户的物理媒体由所有设备共享，各节点地位平等，无中心节点控制。这样的连接布线简单、扩充容易、成本低廉，而且某个节点一旦失效也不会影响其他节点的通信，但使用这种结构必须解决的一个问题是确保端用户发送数据时不会出现冲突。

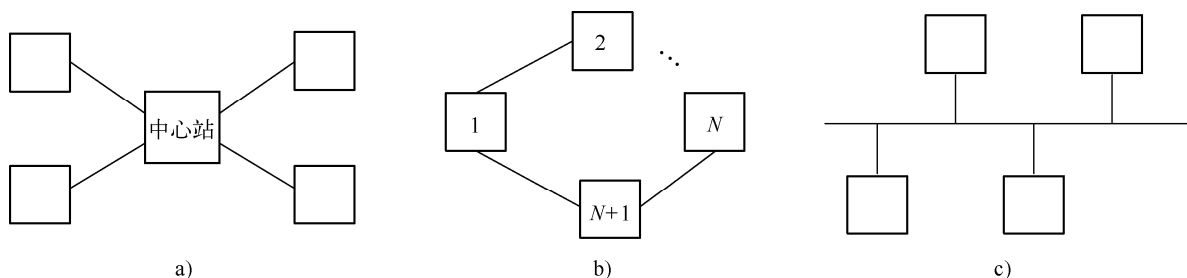


图 2-10 网络拓扑结构图

a) 星形拓扑结构 b) 环形拓扑结构 c) 总线型拓扑结构

## 2. 网络控制方法

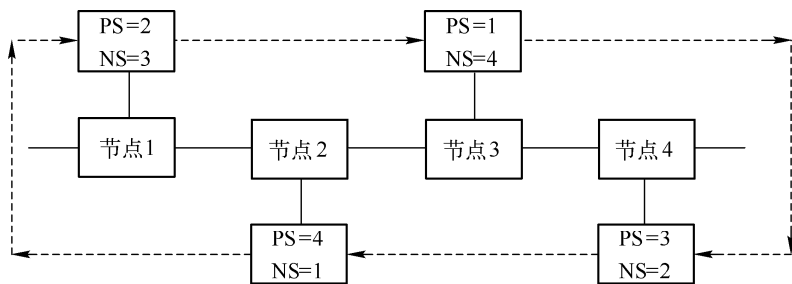
网络控制方法是指在通信网络中使信息从发送装置迅速而正确地传递到接收装置的管理机制。常用的网络控制方法有以下几种。

### (1) 令牌方式

这种传送方式对介质访问的控制权是以令牌为标志的。只有得到令牌的节点才有权控制和使用网络，常用于总线型网络和环形网络结构。

令牌是一组特定的二进制代码，它按照事先排列的某种逻辑顺序沿网络而行，令牌有空、忙两种状态，开始时为空闲；节点只有得到空令牌时才具有信息发送权，同时将令牌置为忙。令牌沿网络而行，当信息被目标节点取走后，令牌被重新置为空闲。

令牌传送实际上是一种按预先的安排让网络中各节点依次轮流占用通信线路的方法，传送的次序由用户根据需要预先确定，而不是按节点在网络中的物理次序传送。如图 2-11 所示，令牌传送次序为节点 1→节点 3→节点 4→节点 2→节点 1。



PS 为前一节点；NS 为下一节点；---→ 为传送方向

图 2-11 令牌传递过程示意图

## (2) 争用方式

这种传送方式允许网络中的各节点自由发送信息，但如果两个以上的节点同时发送信息就会出现线路冲突，故需要加以约束，目前常用的是 CSMA/CD 方式。

CSMA/CD (Carrier Sense Multiple Access/Collision Detect)，即载波监听多路访问/冲突检测，它是一种分布式介质访问控制协议，网络中的各个节点都能独立地决定数据帧的发送与接收。每个站在发送数据帧之前，首先要进行载波监听，只有介质空闲时，才允许发送帧。如果两个以上的站同时监听到介质空闲并发送帧，则会产生冲突现象，会使发送的帧都成为无效帧，发送随即宣告失败。每个站必须有能力随时检测冲突是否发生，一旦发生冲突，则应停止发送，以免介质带宽因传送无效帧而被白白浪费，然后随机延时一段时间后，再重新争用介质，重发送帧。

在点到点链路配置时，如果这条链路是半双工操作，只需使用很简单的机制便可保证两个端用户轮流工作。在一点到多点方式中，对线路的访问由控制端的探询来确定；然而，在总线型网络中，由于所有端用户都是平等的，不能采取上述机制，因此可以采用 CSMA/CD 控制方式来解决端用户发送数据时出现冲突的问题。

CSMA/CD 控制方式的原理比较简单，技术上也容易实现。网络中各工作站处于平等地位，不需要集中控制，不提供优先级控制；但在网络负载增大时，冲突概率增加，发送效率会急剧下降。因此，CSMA/CD 控制方式常用于总线型网络，且通信负荷较轻的场合。

## (3) 主从方式

在这种传送方式中，网络中有主站，主站周期性地轮询各从站节点是否需要通信，被轮询的节点允许与其他节点通信，多用于信息量少的简单系统。主从方式适合于星形网络结构或总线型主从方式的网络拓扑结构。

### 2.3.5 数据交换技术

数据交换技术是网络的核心技术。在数据通信系统中通常采用线路交换、报文交换和分组交换的数据交换方式。

#### 1. 线路交换方式

线路交换是通过网络中的节点在两个站之间建立一条专用的通信线路，从通信资源的分配角度来看，交换就是按照某种方式动态地分配传输线路中的资源。某电话系统的线路连接示意图，如图 2-12 所示。如果主叫端拨号成功，则在两个站之间就建立了一条物理通道。具体过程如下。

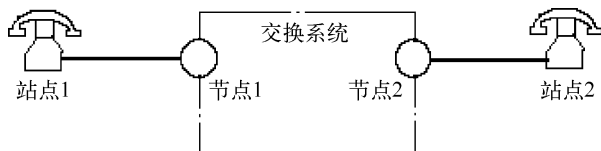


图 2-12 电话系统的线路连接示意图

1) **建立电路**。如果站点 1 发送一个请求到节点 2，请求与站点 2 建立一个连接，那么站点 1 到节点 1 是一条专用线路。在交换机上分配一个专用的通道连接到节点 2、再到站点 2 的通信。至此，就建立了一条从站点 1 出发、经过节点 1、再到站点 2 的通信物理通道。



2) **传输数据**。电路建立成功以后,就可以在两个站点之间进行数据传输,将话音从站点1传送到站点2。这种连接是全双工的,可以在两个方向传输信息。

3) **拆除通道**。在数据传送完成后,就要对建立好的通道进行拆除,这可以由两个站中的任何一个来完成,以便释放专用资源。

线路交换方式的优点是数据传输迅速可靠,并能保持原有序列。缺点是一旦通信双方占有通道后,即使不传送数据,其他用户也不能使用,造成资源浪费。这种方式适用于时间要求高且连续的批量数据传输。

## 2. 报文交换方式

报文交换方式的传输单位是报文,长度不限且可变。报文中包括要发送的正文信息和指明收发站的地址及其他控制信息。数据传送过程采用**存储-转发**的方式,不需要在两个站之间提前建立一条专用通路。在交换装置控制下,报文先存入缓冲存储器中并进行一些必要的处理,当指定的输出线空闲时,再将数据转发出去,例如电报的发送。

报文交换方式的优点是效率高,信道可以复用且需要时才分配信道;可以方便地把报文发送到多个目的节点;建立报文优先权,让优先级高的报文优先传送。缺点是延时长,不能满足实时交互式的通信要求;有时节点收到的报文太多以致不得不丢弃或阻止某些报文;对中继节点存储容量要求较高。

## 3. 分组交换方式

分组交换方式与报文交换方式类似,只是交换的单位为**报文分组**,且限制了每个分组的长度,即将长的报文分成若干个报文组。在每个分组的前面加上一个分组头,用以指明该分组发往何地址,然后由交换机根据每个分组的地址标志,将它们转发至目的地,这些分组不一定按顺序抵达。这样处理可以减轻节点的负担,改善网络传输性能,例如因特网。

分组交换方式的优点是转发延时短,数据传输灵活。由于分组是较小的传输单位,只有出错的分组会被重发而非整个报文,因此大大降低了重发比例,提高了交换速度,而且每个分组可按不同路径和顺序到达。缺点是在目的节点要对分组进行重组,增加了系统的复杂性。

### 2.3.6 差错控制

计算机网络要求高速并且无差错地传递数据信息,但这只是一种比较理想的考虑。一方面,网络是由一个个的实体构成的,这些实体从制造到装配等一系列的过程是很复杂的,在这个复杂的过程中无法保证各个部分都能达到理想的理论值;另一方面,信息在传输过程中会受到诸如突发噪声、随机噪声等干扰的影响而使信号波形失真,从而使接收解调后的信号产生差错。因此,在数据通信过程中需要及时发现并纠正传输中的差错。

差错控制是指在数据通信过程中发现或纠正差错,并把差错限制在尽可能小的、允许的范围之内而采用的技术和方法。

差错控制编码是为了提高数字通信系统的容错性和可靠性,对网络中传输的数字信号所进行的抗干扰编码。其思路是在被传输的信息中增加一些冗余码,利用附加码元和信息码元之间的约束关系进行校验,以检测和纠正错误。冗余码的个数越多,检错和纠错能力就越强。

在差错控制码中,**检错码**是能够自动发现出现差错的编码,**纠错码**是不仅能发现差错而

且能够自动纠正差错的编码。检错和纠错能力是用冗余的信息量和降低系统的效率为代价来换取的。

下面介绍差错控制中常用的几个概念：

- 1) 码长：编码码组的码元总位数称为码组的长度，简称码长。
- 2) 码重：码组中“1”码元的数目称为码组的重量，简称码重。
- 3) 码距：两个等长码组之间对应位上码元不同的数目称为这两个码组的距离，简称码距，又称汉明（Hamming）距离。
- 4) 最小码距：某种编码中各个码组间距离的最小值称为最小码距。
- 5) 编码效率  $R$ ：用差错控制编码提高通信系统的可靠性，是以降低有效性为代价而换来的。定义编码效率  $R = d / (d + r)$  来衡量有效性。其中， $d$  是信息元的个数， $r$  为校验码个数。

差错控制方法分两类，一类是自动检错重发（Automatic Error Request, ARQ），另一类是前向纠错（Forward Error Correction, FEC）。在 ARQ 方式中，当接收端经过检查发现差错时，就会通过一个反馈信道将接收端的判决结果发回给发送端，直到接收端返回接收正确的信号为止，ARQ 方式只使用检错码。在 FEC 方式中，接收端不但能发现差错，而且能确定二进制码元发生错误的位置，从而加以纠正，FEC 方式必须使用纠错码。下面介绍几种常用的差错控制码。

### 1. 常用的简单编码

#### (1) 奇偶校验码

奇偶校验码是一种通过增加冗余位使得码字中“1”的个数为奇数或偶数的编码方法，它是一种检错码。其方法是低 7 位为信息字符，最高位为校验位。这种检错码检错没有办法确定哪一位出错，所以它不能进行错误校正；在发现错误后，只能要求重发。但由于其实现简单，得到了广泛应用。

在奇校验法中，校验位使字符代码中“1”的个数为奇数，例如：1 1010110。接收端按同样的校验方式对收到的信息进行校验，如发送时收到的字符及校验位中“1”的数目为奇数，则认为传输正确，否则认为传输错误。

在偶校验法中，校验位使字符代码中“1”的个数为偶数，例如：0 1010110。接收端按同样的校验方式对收到的信息进行校验，如发送时收到的字符及校验位中“1”的数目为偶数，则认为传输正确，否则认为传输错误。

#### (2) 二维奇偶监督码

二维奇偶监督码又称方阵码，不仅对水平（行）方向的码元，而且还对垂直（列）方向的码元实施奇偶监督，可以检错也可以纠正一些错误。

如图 2-13 所示，将信息码组排列成矩阵，每一个码组写成一行，然后根据奇偶校验原理在垂直和水平两个方向进行校验。

|   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |

图 2-13 方阵码示例

#### (3) 恒比码

码字中“1”的数目与“0”的数目保持恒定比例的码称为恒比码。由于恒比码中，每个码组均含有相同数目的“1”和“0”，因此恒比码又称等重码。这种码在检测时，只要计



算接收码元中“1”的个数是否与规定的相同,就可判断有无错误。

该码的检错能力较强,除对换差错(“1”和“0”成对的产生错误)不能发现外,其他各种错误均能发现。例如,国际上通用的电报通信系统采用7中取3码。

## 2. 线性分组码——汉明码

在线性码中,信息位和监督位由一些线性代数方程联系,或者说,线性码是由一组线性方程构成的。

汉明码也叫海明码,是一种可以纠正一位错的高效率线性分组码。其基本思想是:将待传信息码元分成许多长度为 $k$ 的组,其后附加 $r$ 个用于监督的冗余码元(也称校验位),构成长为 $n=k+r$ 位的分组码。前面介绍的奇偶校验码中,只有一位是监督位,只能代表有错或无错两种信息,并不能指出错码位置。如果选择监督位 $r=2$ ,则其能表示4种状态,其中一种状态用于表示信息是否传送正确,另外3种状态就可能用来指示一位错码的3种不同位置, $r$ 个监督关系式能指示一位错码的 $(2^r-1)$ 个可能位置。

一般地,若码长为 $n$ ,信息位数为 $k$ ,则监督位数 $r=n-k$ 。如果希望用 $r$ 个监督位构造出 $r$ 个监督关系式来指示一位错码的 $n$ 个可能位置,则要求满足以下条件:

$$2^r-1 \geq n \quad \text{或者} \quad 2^r \geq r+k+1$$

汉明码是一种具有纠错功能的纠错码,它能将无效码字恢复成距离它最近的有效码字,但不是百分之百的正确。前面已提到,两个码字的对应位上取值不同的位数称为这两个码字的汉明距离。在一个有效编码集中,任意两个码字的汉明距离的最小值称为该编码集的汉明距离。如果要纠正 $d$ 个错误,则编码集的汉明距离至少应为 $2d+1$ 。

## 2.4 通信模型

### 2.4.1 OSI 参考模型

为了实现不同设备之间的互连与通信,1978年国际标准化组织(ISO)提出了一个试图使各种计算机在世界范围内互连为网络的标准框架,即开放系统互连(Open System Interconnection, OSI)参考模型,1983年成为正式国际标准(ISO 7498)。

OSI参考模型是计算机通信领域的开放式标准,是用来指导生产厂家和用户共同遵循的规范,任何人都可免费使用,而使用这个规范的系统也必须向其他使用这个规范的系统开放。OSI参考模型并没有提供一个可以实现的方法,它是一个在制定标准时所使用的概念性框架,设计者可根据这一框架,设计出符合各自特点的网络。

OSI参考模型将计算机网络的通信过程分为7个层次,每层执行部分通信功能,如表2-2所示。“层”这个概念包含了两个含义,即问题的层次及逻辑的嵌套关系;这种关系类似信件中采用多层信封把信息包装起来:发信时要由里往外包装,收信后要由外到里拆封,最后才能得到所传送的信息。每一层都有双方相应的规则,相当于每一层信封上都有相互理解的标志,否则信息就无法传递到预期的目的地。每一层依靠相邻的低一层完成较原始的功能,同时又为相邻的高一层提供服务;邻层之间的约定称为接口,各层约定的规则总和称为协议,只要相邻层的接口一致,就可以进行通信。第1层~第3层



为介质层，负责网络中数据的物理传输；第4层~第7层为高层或主机层，用于保证数据传输的可靠性。

表 2-2 OSI 模型分层简况

| 层 号   | 层 名   | 英 文 名          | 接 口 要 求 | 工 作 任 务 |
|-------|-------|----------------|---------|---------|
| 第 1 层 | 物理层   | Physical layer | 物理接口定义  | 比特流传输   |
| 第 2 层 | 数据链路层 | Data Link      | 介质访问方案  | 成帧、纠错   |
| 第 3 层 | 网络层   | Network        | 路由器选择   | 选线、寻址   |
| 第 4 层 | 传输层   | Transport      | 数据传输    | 收发数据    |
| 第 5 层 | 会话层   | Session        | 对话结构    | 同步      |
| 第 6 层 | 表示层   | Presentation   | 数据表达    | 编译      |
| 第 7 层 | 应用层   | Application    | 应用操作    | 协调、管理   |

在模型的7层中，物理层是通信的硬件设备，由它完成通信过程；从第7层到第2层的信息并没有进行传送，只是为传送做准备，这种准备由软件进行处理，直到第1层才靠硬件真正进行信息的传送。下面简单介绍 OSI 参考模型的7个层次的功能或工作任务。

### 1. 物理层

物理层是必不可少的，它是整个开放系统的基础，负责设备间接收和发送比特流，提供为建立、维护和释放物理连接所需要的机械、电气、功能与规程的特性。例如，使用什么样的物理信号来表示数据“0”和“1”，数据传输是否可同时在两个方向上进行等。

### 2. 数据链路层

数据链路层也是必不可少的，它被建立在物理传输能力的基础上，以帧为单位传输数据。它负责把不可靠的传输信道改造成可靠的传输信道，采用差错检测和帧确认技术，传送带有校验信息的数据帧。

### 3. 网络层

网络层提供逻辑地址和路由选择。网络层的作用是确定数据包的传输路径，建立、维持和拆除网络连接。

### 4. 传输层

传输层属于 OSI 参考模型中的高层，解决的是数据在网络之间的传输质量问题，提供可靠的端到端的数据传输，保证数据按序可靠、正确的传输。这一层主要涉及网络传输协议，提供一套网络数据传输标准，如 TCP、UDP。

### 5. 会话层

会话是指请求方与应答方交换的一组数据流。会话层用来实现两个计算机系统之间的连接，建立、维护和管理会话。

### 6. 表示层

表示层主要处理数据格式，负责管理数据编码方式，它是 OSI 参考模型的翻译器，该层从应用层取得数据，然后把它转换为计算机应用层能够读取的格式，如 ASCII、MPEG 等格式。



## 7. 应用层

应用层是 OSI 参考模型中最靠近用户的一层，提供应用程序之间的通信，其作用是实现应用程序之间的信息交换、协调应用进程和管理系统资源，如 QQ 等。

两个相互通信的系统应该具有相同的层次结构，不同节点的同等层次具有相同的功能，并按照协议实现同等层之间的通信。如果把要传送的信息称为“报文”，则每一层上的标记称为“报头”，数据封装和拆封过程如下。

当信息发送时，从第 7 层到第 2 层并没有进行站与站的信息传送，而是在进行软件方面的处理，直到第 1 层才靠传输介质将信息真正传送出去，即物理层把封装后的信息由物理层放到通信线路上进行传输；当信息到达接收站后，按照与封装相反的顺序进行数据解封，每经过一层就去掉一个报头，到第 7 层之后，所有的报头、报尾都去掉了，只剩数据或报文本身；至此，站与站之间的通信结束。

OSI 参考模型是一个理论模型，在实际环境中并没有一个真实的网络系统与之完全相对应，它更多地被作为分析和判断通信网络技术的依据。多数应用只是将 OSI 模型与应用的协议进行大致的对应，对应于 OSI 的某层或包含某层的功能。

图 2-14 为局域网体系结构 IEEE 802 与 OSI 参考模型的对应关系，这里只定义了数据链路层和物理层，数据链路层又分为两个子层：介质访问控制（Medium Access Control, MAC）层和逻辑链路控制（Logical Link Control, LLC）层。MAC 子层解决网络上所有节点共享一个信道所带来的信道争用问题；LLC 子层把要传输的数据组帧，并解决差错控制和流量控制问题，从而实现可靠的数据传输。

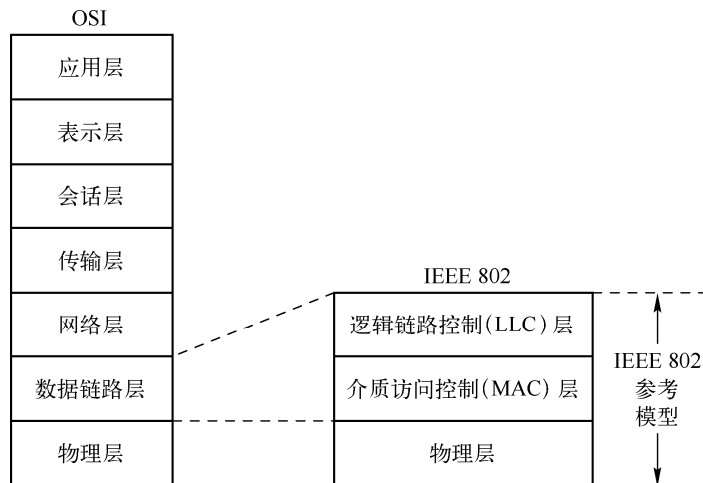


图 2-14 IEEE 802 与 OSI 参考模型的对应关系

图 2-15 为 TCP/IP 与 OSI 参考模型的对应关系。传输控制协议/互联网协议（Transmission Control Protocol/Internet Protocol, TCP/IP）是针对 Internet 开发的一种体系结构和协议标准，目的在于解决异构计算机网络的通信问题。TCP/IP 模型采用 4 层的分层体系结构，由下向上依次是网络接口层、网际层、传输层和应用层。其中，TCP 提供了一种可靠的数据交互服务；IP 规定了数据包传送的格式。TCP/IP 是互联网上事实上的标准协议。

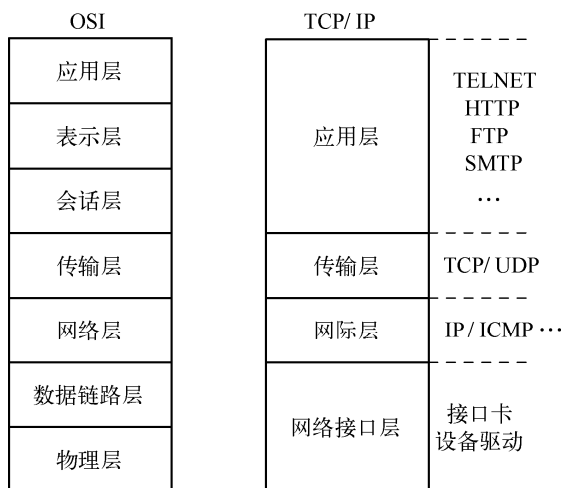


图 2-15 TCP/IP 与 OSI 参考模型的对应关系

## 2.4.2 现场总线通信模型

现场总线是工业控制现场的底层网络。工业生产现场存在大量的传感器、控制器、执行器等设备，它们被零散地分布在一个较大的工作范围内。对于由这些设备组成的工业控制底层网络来说，某个节点面向控制的信息量并不大，信息传输的任务也相对比较简单，但系统对实时性、快速性的要求较高。对于这样的控制系统要构成开放式的互联系统，需要考虑以下几个重要问题。

1) 采用什么样的通信模型合适？是采用 OSI 的完全模型，还是在此基础上做进一步的简化？

2) 采用什么样的协议合适？是否需要实现 OSI 的全部功能？

3) 所选择的通信模型能适应生产现场的环境要求和系统性能要求吗？

虽然 7 层结构的 OSI 参考模型所支持的通信功能相当强大，但对于只需要完成简单通信任务的工业控制底层网络而言，完全模型显得过于复杂，不仅网络接口造价高，而且会由于层间操作与转换复杂导致通信时间响应过长。因此，现场总线系统为了满足生产现场的实时性、快速性要求，也为了实现工业网络的低成本，对 OSI 参考模型进行了简化和优化，除去了实时性不强的中间层，并增加了用户层，构成了现场总线通信系统模型。

目前，各个公司生产的现场总线产品虽然采用了不同的通信协议，但是各公司在制定自己的通信协议时，都参考了 OSI 的 7 层模式。典型的现场总线通信模型如图 2-16 所示，它采用 OSI 模型中的 3 个典型层：物理层、数据链路层和应用层，省去了中间的 3~6 层部分，同时考虑到现场设备的控制功能和具体应用，增设了第 8 层，即用户层。这种模型具有结构简单、执行协议直观、价格便宜等优点，也能满足工业现场应用的性能要求。它是 OSI 模型的简化形式，流量与差错控制都在数据链路层中进行，因而与 OSI 模型并不完全一致。

现场总线通信模型的主要特点总结如下。



图 2-16 现场总线通信模型



1) 简化了 OSI 参考模型。通常只采用 OSI 参考模型的第 1 层（物理层）、第 2 层（数据链路层）及最高层（应用层），以便简化通信模型结构、缩短通信开销、降低系统成本及提高系统的实时性。

2) 采用相应的补充方法实现被删除的 OSI 各层功能，并增设了用户层。

3) 现场总线通信模型通信数据的信息量较小。相对于其他通信网络而言，通信模型相对简单，但结构更加紧凑，实时性更好，通信速率更快。

4) 多种现场总线并存，并采用不同的通信协议。但在应用与发展中都已形成自己的特点和应用领域。

总之，开放系统互连模型是现场总线技术的基础，现场总线参考模型既要遵循开放系统集成原则，又要充分兼顾现场总线控制系统应用的特点和不同控制系统提出的相应要求。

## 2.5 网络互联设备

网络互联是将两个以上的网络系统，通过一定的方法，用一种或多种网络互联设备相互连接起来，构成更大规模的网络系统，以便更好地实现网络数据的资源共享。相互连接的网络可以是同种类型的网络也可以是运行不同网络协议的异型系统。网络互联不能改变原有网络内的网络协议、通信速率、软硬件配置等，但通过网络互联技术可以使原先不能相互通信和共享资源的网络之间有条件实现相互通信和信息共享。

采用中继器、集线器、网卡、交换机、网桥、路由器、防火墙、网关等网络互联设备可以将不同网段或子网连接成企业应用系统。

### 1. 中继器

中继器工作在物理层，是一种最为简单但也是用得最多的互联设备。它负责在两个节点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。中继器由于不对信号进行校验等其他处理，因此即使是差错信号，中继器也照样整形放大。

中继器一般有两个端口，用于连接两个网段，且要求两端的网段具有相同的介质访问方法。

### 2. 集线器

集线器（hub）工作在物理层，是对网络进行集中管理的最小单元，对传输的电信号进行整形、放大，相当于具有多个端口的中继器。

### 3. 网络接口卡

网络接口卡，简称网卡。主要工作在数据链路层，不仅可以实现与局域网通信介质之间的物理连接和电信号匹配，还可以实现数据链路层数据帧的封装与拆封、数据帧的发送与接收、物理层的介质访问控制、数据编码与解码以及数据缓存等功能。

网卡的序列号是网卡的物理地址，即 MAC 地址，用以标识该网卡的唯一性。

### 4. 交换机

交换机工作在数据链路层，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行数据转发，并将 MAC 地址与对应的端口记录在自己内部的一个地址表中。数据帧转发前先送入交换机的内部缓冲，可对数据帧进行差错检查。



## 5. 网桥

网桥，也叫桥接器。主要工作在数据链路层，根据 MAC 地址对帧进行存储转发。它可以有效地连接两个局域网（Local Area Network, LAN），使本地通信限制在本网段内，并转发相应的信号至另一网段。网桥通常用于连接数量不多的、同一类型的网段。网桥将一个较大的 LAN 分成子段，有利于改善网络的性能、可靠性和安全性。

网桥一般有两个端口，每个端口均有自己的 MAC 地址，分别桥接两个网段。

## 6. 路由器

路由器工作在网络层，在不同网络之间转发数据单元。因此，路由器具有判断网络地址和选择路径的功能，能在多网络互连环境中建立灵活的连接。

路由器最重要的功能是路由选择，为经由路由器转发的每个数据包寻找一条最佳的转发路径。路由器比网桥更复杂、管理功能更强大，同时更具灵活性，经常被用于多个局域网、局域网与广域网以及异构网络的互联。

## 7. 防火墙

防火墙一方面用于阻止来自因特网的对受保护网络的未经授权或未经验证的访问，另一方面允许内部网络的用户对因特网进行 Web 访问或收发电子邮件等，也可以作为访问因特网的权限控制关口，如授权组织内特定的人访问因特网。

## 8. 网关

网关工作在传输层或以上层次，是最复杂的网络互联设备。网关就像一个翻译器，当对使用不同通信协议、数据格式甚至网络体系结构的网络互联时，需要使用这样的设备，因此又被称作协议转换器。与网桥只是简单地传达信息不同，网关对收到的信息需要重新打包，以适应目的端系统的需求。

网关具有从物理层到应用层的协议转换能力，主要用于异构网络的互联、局域网与广域网的互联，不存在通用的网关。

# 2.6 现场总线控制网络

## 2.6.1 现场总线网络节点

现场总线控制网络用于完成各种数据采集和自动控制任务，是一种特殊的、开放的计算机网络，它是工业企业综合自动化的基础。从现场控制网络节点的设备类型、传输信息的种类、网络所执行的任务、网络所处的环境等方面来看，都有别于其他计算机构成的数据网络。

现场总线控制网络可以通过网络互联技术实现不同网段之间的网络连接与数据交换，包括在不同传输介质、不同传输速率、不同通信协议的网络之间实现互联，从而更好地实现现场检测、数据采集、控制和执行以及信息的传输、交换、存储与利用的一体化，满足用户的需求。

现场总线网络的节点常常分散在生产现场，大多是具有计算与通信能力的智能测控设备。它们可能是普通计算机网络中的个人计算机或其他种类的计算机、操作站等设备。也可能是具有嵌入式 CPU，但功能比较单一、计算或其他能力远不及普通计算机，且没有键盘、



显示等的人机交互接口。也有的设备甚至不带有 CPU，只带有简单的通信接口。

例如，具有通信能力的现场设备有：条形码阅读器、各类智能开关、可编程序控制器、监控计算机、智能调节阀、变频器、机器人等，这些都可以作为现场总线控制网络的节点使用。由于受到制造成本等因素的影响，作为现场总线网络节点的设备，在计算能力等方面一般比不上普通的计算机。

现场总线控制网络就是把单个分散的、有通信能力的测控设备作为网络节点，按照总线型、星形、树形等网络拓扑结构连接而成的网络系统。如图 2-17 所示的总线型控制网络连接，使得各个节点之间可以相互沟通信息、共同配合完成系统的控制任务。

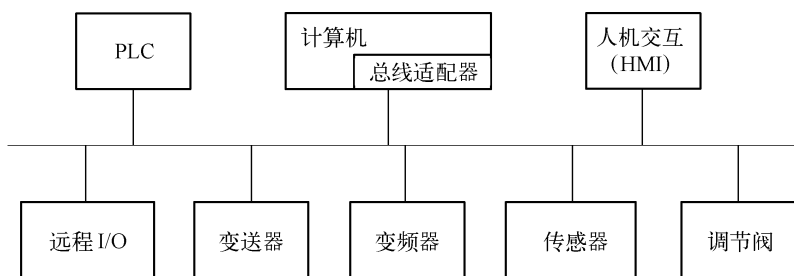


图 2-17 现场总线控制网络连接示意图

### 2.6.2 现场总线控制网络的任务

现场总线控制网络主要完成以下任务。

- 1) 将控制系统中现场运行的各种信息传送到控制室，使现场设备始终处于[远程监视](#)之中。例如，在控制室监视生产现场阀门的开度、开关的状态、运行参数的测量值及现场仪表的工作状况等信息。
- 2) 控制室将各种控制、维护、参数修改等命令信息送往位于生产现场的测量控制设备中，使得生产现场的设备处于[可控状态](#)之中。
- 3) 与操作终端、上层管理网络实现[数据传输与信息共享](#)。

此外，现场总线控制网络还要面临工业生产的高温高压、强电磁干扰、各种机械振动及其他恶劣工作环境，因此要求现场总线控制网络能适应各种可能的工作环境。

正是由于现场总线控制网络要完成的工作任务和所处的工作环境，使得它具有许多不同于普通计算机网络的特点。

影响控制网络性能的主要因素有网络的拓扑结构、传输介质的种类与特性、介质访问方式、信号传输方式以及网络监控系统等。为了适应和满足自动控制任务的需求，在开发控制网络技术及设计现场总线控制网络系统时，应该着重于满足控制的实时性、可靠性以及工业环境下的抗干扰性等控制要求。

### 2.6.3 控制网络的安全问题

随着控制网络中智能设备、计算机等智能节点的使用，以及控制网络与企业管理层网络及其他业务应用的集成，控制网络的信息交换需求与共享范围也在不断扩大，这种交换和共享信息的能力一方面扩展了控制网络的功能，另一方面由于工业领域的合作联盟、外包服务及 IP 的使用等因素，使得工业自动化控制系统与现场设备在网络层可能会受到同商业系统



一样的攻击；再加上近年来对商业和个人计算机的恶意攻击显著增加，因特网上用于自动攻击的工具又随处可见，因此，控制网络的应用和信息向商业领域的延伸都大大增加了工业自动化控制系统运行的风险。

由于工业自动化控制系统的设备是直接和工艺过程相联系的，信息安全一旦遭到破坏，就可能会造成商业机密泄露、信息传送中断，还可能会带来潜在的对人员或生产造成的损失、环境破坏以及危及运行安全等严重后果，因此工业控制系统的信息安全问题已经受到越来越广泛的关注，控制网络对于信息安全的需求也显得越来越重要。

## 2.7 思考与练习

1. 什么是总线？总线主设备和从设备各起什么作用？
2. 总线上的控制信号有哪几种？各起什么作用？
3. 总线的寻址方式有哪些？各有什么特点？
4. 数据通信系统由哪些设备组成？各起什么作用？
5. 试比较串行通信和并行通信的优缺点。
6. 串行通信接口标准有哪些？试分别阐述其电气特性。
7. 常用的网络控制方法有哪几种？
8. 通常使用的数据交换技术有几种？它们各有什么特点？
9. 曼彻斯特编码波形的跳变有几层含义？
10. 什么是差错控制？列举两种基本的差错控制方式。
11. 采用光缆传输数据有哪些优势？
12. 为什么要引进 OSI 参考模型？它能解决什么问题？
13. 简述 OSI 七层模型的结构和每一层的作用。
14. 列出几种网络互联设备，并说明其功能。
15. 集线器、交换机和路由器分别工作在 OSI 参考模型的哪一层？
16. 什么是防火墙？它在网络系统中起什么作用？
17. 现场总线通信模型有什么特点？
18. 试阐述现场总线控制网络的特点和它承担的主要任务。

## 第3章 PROFIBUS 总线及其应用

PROFIBUS 是一种应用广泛的、开放的、不依赖于设备生产商的现场总线标准，适合于快速、时间要求严格的应用和复杂的通信任务。其通信本质是 RS-485 串口通信，按照对应用环境的要求可分为 PROFIBUS-DP 和 PROFIBUS-PA 两种互相兼容的规约。

PROFIBUS 的网络设备主要有：PROFIBUS 接口、PROFIBUS 插头、有源终端电阻、通信介质、中继器以及光链路模块等；PROFIBUS 设备根据其在网络中所起的作用不同可分为 1 类主站、2 类主站和从站；其传输技术有用于 DP 的 RS-485 技术和光纤传输技术，用于 PA 的 IEC 1158-2 传输技术；总线存取控制方式有主站间的令牌传递方式和主从站间的主从通信方式。

### 学习目标

- ◇ 了解 PROFIBUS 总线的概念、分类及传输技术。
- ◇ 了解 GSD 文件及更新方法。
- ◇ 学会 PROFIBUS 控制系统的硬件配置及组态。
- ◇ 掌握简单 PROFIBUS 控制系统的设计与实现方法。

## 3.1 PROFIBUS 总线基础

### 3.1.1 PROFIBUS 总线及分类

2001 年，PROFIBUS 成为中国机械行业推荐标准 JB/T 10308—2001；2006 年成为我国第一个工业通信领域现场总线技术国家标准 GB/T 20540—2006。

目前，世界上许多自动化设备制造商都为其生产的设备提供了 PROFIBUS 接口，PROFIBUS 现场总线已广泛应用于加工制造、过程控制、楼宇自动化、交通电力等应用领域。

PROFIBUS 现场总线根据应用的特点和用户不同的需要，可分为 PROFIBUS-DP、PROFIBUS-PA、PROFIBUS-FMS 三个互相兼容版本的通信协议。

1) PROFIBUS-DP (DP 是 Distributed Periphery 的缩写，即分布 I/O 系统) 主要用于自动化系统中单元级和现场级通信；通过两线制线路或光缆联网，可实现 9.6 kbit/s~12 Mbit/s 的数据传输速率；网络符合 IEC 61158-2/EN 61158-2 标准，采用混合协议令牌总线和主站/从站架构。

2) PROFIBUS-PA (PA 是 Process Automation 的缩写，即过程自动化) 用于工业现场控制的过程自动化，是以 PROFIBUS-DP 为基础，增加了 PA 行规以及相应的传输技术，使 PROFIBUS 能更好地满足各种过程控制的要求。通信采用扩展的 PROFIBUS-DP 协议，传输

技术采用 IEC6 1158-2，即提供标准的本质安全的传输技术；网络可基于屏蔽双绞线线路进行本质安全设计，数据传输速率为 31.25 Mbit/s，一般用于安全性要求较高的场合及由总线供电的站点。

3) PROFIBUS-FMS (FMS 是 Fieldbus Message Specification 的缩写，即现场总线信息规范) 用于车间级监控网络，主要解决车间级通用性通信任务，可以提供大量的通信服务，完成中等速度的循环和非循环通信任务，多用于纺织工业、楼宇自动化、电气传动、传感器和执行器、PLC 等自动化控制，一般构成实时多主站网络系统，是一种令牌结构、实时的多主网络。对于 FMS 而言，它考虑的主要是系统功能而不是响应时间，主要用于大范围的、复杂的通信系统。

随着现场总线应用领域的不断扩大和工业以太网的发展，PROFIBUS 技术也在不断发生变化，例如 PROFIBUS-FMS 目前已不再使用，而 PROFIBUS-DP 和 PROFIBUS-PA 的应用则越来越多，另外像 PROFIdrive、PROFIsafe 等新的行规随着应用的增加也在逐渐普及。

### 3.1.2 PROFIBUS 的通信协议

#### 1. PROFIBUS 的协议结构

PROFIBUS 是根据 ISO 7498 国际标准，以 OSI 参考模型为基础，并增加了用户层。第 1 层为物理层，用来定义物理传输特性；第 2 层为数据链路层，用来解决两个相邻节点之间的通信问题；第 3~7 层未加描述；用户层用来定义应用功能。PROFIBUS 的协议结构示意图如 3-1 所示。

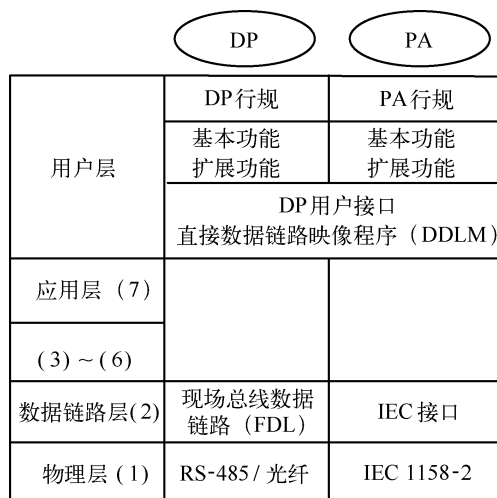


图 3-1 PROFIBUS 的协议结构示意图

#### (1) PROFIBUS-DP

PROFIBUS-DP 定义了第 1、2 层和用户接口层。直接数据链路映像程序 (DDLML) 提供对第 2 层的访问，第 3 层至第 7 层未加描述，这种简化的协议结构保证了数据传输的快速性和有效性。该模型提供了 RS-485 传输技术和光纤传输技术；详细说明了各种不同 PROFIBUS-DP 设备的设备行为；定义了用户、系统以及不同设备可以调用的应用功能。特别适合可编程控制器与现场分散的 I/O 设备之间的快速通信。

#### (2) PROFIBUS-PA

PROFIBUS-PA 采用扩展的 PROFIBUS-DP 协议进行数据传输，另外，它还使用了描述现

场设备行为的 PA 规范。根据 IEC 1158-2 标准，这种传输技术可确保其本质安全，并使现场设备通过总线供电。

通过 DP/PA 耦合器和 DP/PA LINK 连接器，可以将 PROFIBUS-PA 设备很方便地集成到 PROFIBUS-DP 网络上，如图 3-2 所示。DP/PA 耦合器用于在 DP 和 PA 之间传递物理信号，适用于简单网络与运行时间要求不高的场合，分为两种类型：非本质安全型和本质安全型。

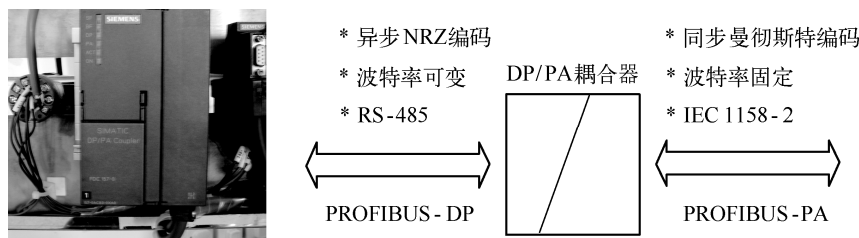


图 3-2 用耦合器转换协议

PA 现场设备还可以通过 DP/PA 链路设备连接到 DP 网络上。DP/PA 链路设备应用于大型网络时，根据网络复杂程度和处理时间要求的不同，会有不止一个链路设备连接到 DP。DP/PA 链路设备既作为 DP 网段的从站又作为 PA 网段的主站，耦合网络上的所有数据通信；这意味着在不影响 DP 性能的情况下，DP/PA 链路设备将 DP 和 PA 结合起来，由于每个链路设备可以连接多台设备，而链路设备只占用 DP 的一个站地址，因此整个网络所能容纳的设备数量大大增加。

PROFIBUS-PA 是为满足过程自动化工程中高速、可靠的通信要求而特别设计的。用 PROFIBUS-PA 可以把传感器和执行器连接到现场总线上，即使在防爆区域的传感器和执行器也是这样。

## 2. 现场总线数据链路层

从图 3-1 可以看到，PROFIBUS 协议的第 2 层为现场总线数据链路（Fieldbus Data Link, FDL）层。该层协议可以处理两个由物理通道直接相连的邻接站之间的通信，定义为数据安全性、传输协议、报文处理及总线访问控制层；协议目的在于提高数据传输的效率，为其上层提供透明、无差错的通道服务。

数据链路层的报文格式保证了传输的高度安全性。所有报文均具有汉明距离  $HD=4$ ，其含义是在数据报文中能同时发送 3 种错误位，这符合国际标准 IEC 870-5.1 系列规约，数据报文选择特殊的开始和结束标识符，并运用无间隙同步、奇偶校验位和控制位；可检测下列差错类型：

- 1) 字符格式错误（奇偶校验、溢出、帧错误）。
- 2) 协议错误。
- 3) 开始和结束标识符错误。
- 4) 帧检查字节错误。
- 5) 报文长度错误。

在第 2 层中，除逻辑上点到点的数据传输之外，还允许用广播和群播通信的多点传送。广播通信就是一个主站点把信息发送到其他所有站点，而收到数据则不需要应答；群播是指一个主站向一个预先确定的站发送无须应答的报文。

### 3. 总线存取协议

PROFIBUS-DP 和 PROFIBUS-PA 均使用一致的总线存取协议，通过 OSI 参考模型的第 2 层（数据链路层）来实现。介质存取控制（Medium Access Control, MAC）必须确保在任何时刻只能由一个站点发送数据。PROFIBUS 协议的设计要满足介质控制的两个基本要求：其一，同一级的 PLC 或主站之间的通信必须使每一个主站在确定的时间范围内能获得足够多的机会来处理它自己的通信任务；其二，主站和从站之间应尽可能快速而又简单地完成数据的实时传输。为此，PROFIBUS 使用混合的总线存取控制机制来实现上述目标，包括用于主站之间通信的令牌传递方式和用于主站与从站之间通信的主从方式。

当一个主站获得令牌时，它就可以拥有主从站通信的总线控制权，而且此地址在整个总线上必须是唯一的。在一个总线内，最大可使用的站地址范围是在 0~126 之间，也就是说，一个总线系统最多可以有 127 个节点。

这种总线存取控制方式可以有以下 3 种系统配置。

- 1) 纯主-主系统（令牌传递方式）。
- 2) 纯主-从系统（主从方式）。
- 3) 两种方式的组合。

PROFIBUS 的总线存取机制与所使用的传输介质无关，即不论使用的是铜质电缆还是光纤电缆，效果是一样的。

#### （1）令牌总线通信过程

连接到 PROFIBUS 网络的主站按它的总线地址的升序组成一个逻辑令牌环，PROFIBUS 系统的多主结构示意图如图 3-3 所示。在逻辑令牌环中控制令牌按照事先给定的顺序从一个站传递到下一个站，令牌提供控制总线的权力，并用特殊的令牌帧在主站点间进行传递。具有最高站地址（Highest Address Station, HAS）的主站点例外，它只把令牌传递给具有最低总线地址的主站点，以此使逻辑令牌环闭合。令牌环调度要保证每个主站有足够的时间来完成它的通信任务。令牌经过所有主站点轮转一次所需时间叫作实际令牌循环时间（TRR），每一次令牌交换都会计算产生一个新的 TRR；用目标令牌时间（TTR）来规定现场总线系统中令牌轮转一次所允许的最长时间，这个时间是可以调整的；一个主站在获得令牌后，就是通过计算  $TTR - TRR$  来确定自己持有令牌的时间（TTH）。

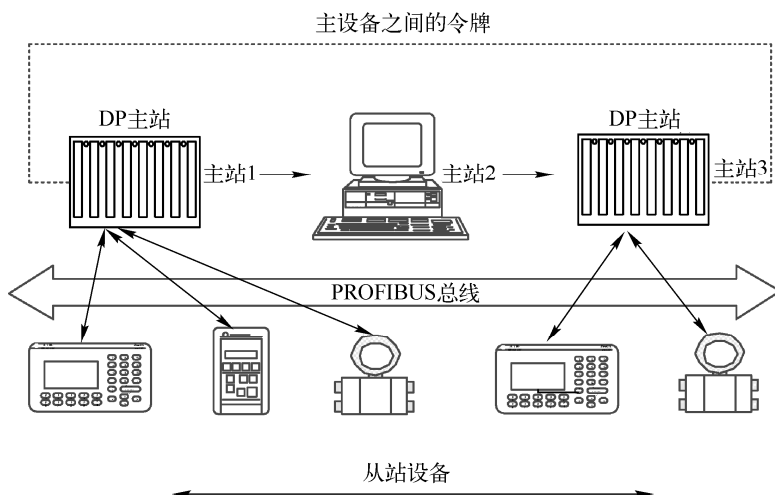


图 3-3 PROFIBUS 系统的多主结构示意图



在总线初始化和启动阶段，MAC 通过辨认主站点来建立令牌环。为了管理控制令牌，MAC 程序首先自动地判定总线上所有主站点的地址，并将这些节点及它们的节点地址都记录在活动主站表（List of Active Master Stations, LAS）中。对于令牌管理而言，有两个地址概念特别重要：一个是前一站（Previous Station, PS）节点的地址，即下一站是从此站接收到令牌的；另一个是下一站（Next Station, NS）节点的地址，即令牌传递给此站。

在运行期间，为了从令牌环中去掉有故障的主站点或增加新的主站点到令牌环中而不影响总线上的数据通信，也需要用到 LAS。若一个主站从 LAS 中自己的前一站（PS）节点收到令牌，则保留令牌并使用总线；若主站收到的令牌帧不是从前一站节点发出的，将认为是一个错误而不接收令牌；如果此令牌帧被再次收到，该主站将认为令牌环已修改，接收令牌并修改自己的 LAS。

## （2）主从通信过程

一个网络中有若干个从站，而它的逻辑令牌环只含一个主站，这样的网络就称为纯主-从系统，PROFIBUS 主从通信过程如图 3-4 所示，此系统不存在令牌的传递。主从通信允许主站控制它自己所控制的从站，使得从站做出相应的响应；主站要与每一个从站建立一条数据链路；主站可以发送信息给从站或者获取从站信息。

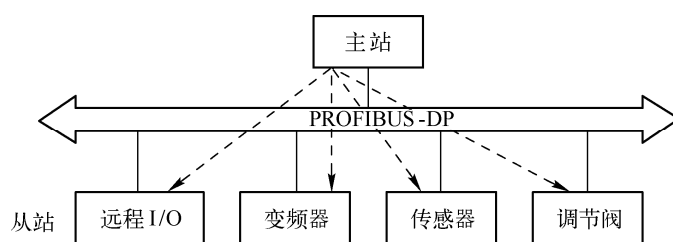


图 3-4 PROFIBUS 主从通信过程

主从（Master-Slave, MS）通信方式是 PROFIBUS-DP 主站与智能从站之间的数据交换方式，可以由 PLC 的操作系统周期性的自动完成，不需要用户程序进行控制。但用户必须对主站和智能从站之间的通信连接和数据交换区进行配置。

在分布式 PLC 系统中，PLC 可以被设为主站，通过 PROFIBUS-DP 总线来连接分布式 I/O 从站，如 ET200B 紧凑型 DP 从站、ET200M 模块式 DP 从站等，这些从站实质上只是带有 PROFIBUS-DP 通信处理器的 I/O 模块，称为标准从站或普通从站。标准从站的 I/O 被直接并入 DP 主站的 I/O 地址区，使用时可以像主站本身的 I/O 模块一样直接访问标准从站的输入/输出。

对于带有多台 PLC 的控制系统或其他带有 CPU、存储器等部件的独立控制设备，可以实现不同子任务的独立和有效处理。同时，整个控制系统为了实现分散控制、集中管理，将这些设备都挂接在 PROFIBUS-DP 网络上。这些独立的控制设备在 DP 网络中被称为智能从站。

智能从站本身具有独立的 I/O 地址，这些地址可能会与主站的 I/O 地址相同，因此，DP 主站不能直接访问智能从站的输入/输出，而是需要建立 I/O 地址的传输空间，并由智能从站的 CPU 负责处理地址转换工作。



### (3) 两种方式的组合

一个 DP 系统可能是多主结构,这意味着一条总线上已经连接了几个主站节点,主站间采用逻辑令牌环、主从站间采用主从通信的方式传输。

令牌传递程序保证每个主站在一个确切规定的时间内得到总线控制权;主站得到总线控制权时,可与从站进行主从通信,对从站进行分时轮询传输信息。

在图 3-3 中,总线系统由 3 个主站和 5 个从站构成。3 个主站之间构成令牌逻辑环:主站 1→主站 2→主站 3→主站 1。当其中一个主站得到令牌报文后,该主站就在一定时间内执行主站工作;在这段时间内,它可依照主从关系通信表与所有从站通信,也可依照主-主通信关系表与所有主站通信。如果主站 1 需要向主站 3 发送数据,当令牌传递到主站 1 时,主站 1 将要发送的数据按照一定的格式发往主站 2,主站 2 将本站地址与接收到的帧信息中的目的地址进行比较,地址不同则主站 2 将帧信息继续传递到主站 3;主站 3 将本站地址与接收到的帧信息中的目的地址进行比较,比较后由于地址相同则主站 3 获得了总线控制权,此时主站 3 与主站 1 进行数据传递,同时也可以与它所挂接的两个从设备进行通信。当主站 3 没有需要发送的帧或在规定时间内发送完了所需发送的帧,或者主站 3 的控制时间终了时,它就将主站令牌传递给主站 1。

## 3.2 PROFIBUS 的传输技术

现场总线系统的应用在较大程度上取决于采用哪种传输技术,而且既要考虑传输的拓扑结构、传输速率、传输距离和传输的可靠性等通用要求,还要考虑成本低廉、使用方便等因素。在过程自动化的应用中,为了满足本质安全的要求,数据和电源还必须使用同一根传输媒介,因此单一的传输技术不可能满足以上所有要求。

在通信模型中,物理层直接和传输介质相连,规定了线路传输介质、物理连接的类型以及电气、功能等特性,提供了以下 3 种数据传输类型。

- 1) 用于 DP 的 RS-485 传输技术。
- 2) 用于 DP 的光纤传输技术。
- 3) 用于 PA 的 IEC 1158-2 传输技术。

### 3.2.1 RS-485 传输技术

#### 1. RS-485 传输技术的特点

RS-485 是一种简单的、低成本的传输技术,其传输过程是建立在半双工、异步、无间隙同步化的基础上,数据的发送采用 NRZ 编码,这种传输技术通常称之为 H2。网络连接情况如图 3-5 所示,具有以下特点。

1) **网络拓扑**:所有设备都连接在总线结构中,每个总线段的开头和结尾均有一个终端电阻。为确保操作运行不发生误差,两个总线终端电阻必须要有电源。

2) **传输介质**:双绞屏蔽电缆,也可取消屏蔽,取决于电磁干扰环境即电磁兼容性(Electro Magnetic Compatibility, EMC)的条件。

3) **站点数**:每个总线段最多可以连接 32 个站,如果站数超过 32 个或需要扩大网络区域,则需要使用中继器来连接各个总线段。使用中继器时最多可用到 127 个站,串联的中继

器一般不超过 3 个。

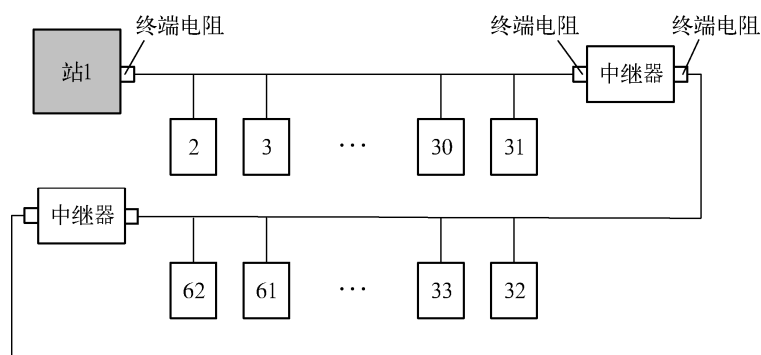


图 3-5 使用中继器连接各总线段

4) **插头连接**：采用 9 脚 D 型插头，插座被安装在设备上。9 脚 D 型插头和插座外观如图 3-6a、b 所示，如果其他连接器能提供如表 3-1 所示的必要的命令信号，则也可以被使用。

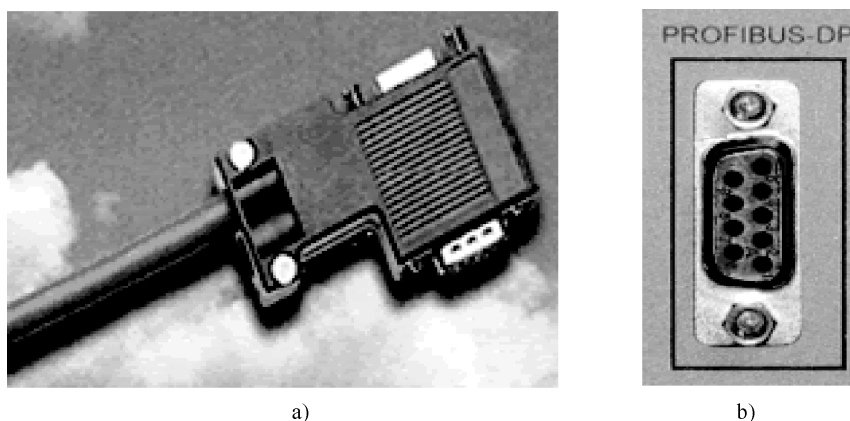


图 3-6 9 脚 D 型插头和插座外观示意图

a) 9 脚 D 型插头 b) 插座外观

表 3-1 9 脚 D 型连接器的针脚分配

| 引脚号 | 信号        | 信号含义           |
|-----|-----------|----------------|
| 1   | Shield    | 屏蔽/保护地         |
| 2   | M24       | 24 V 输出电压的地    |
| 3   | RxD/TxD-P | 接收数据/发送数据（正）   |
| 4   | CNTR-P    | 中继器控制信号（正方向控制） |
| 5   | DGND      | 数据基准电压         |
| 6   | VP        | 供电电压           |
| 7   | P24       | 输出电压 24 V      |
| 8   | RxD/TxD-N | 接收数据/发送数据（负）   |
| 9   | CNTR-N    | 中继器控制信号（负方向控制） |

5) **传输速率**：可以在 9.6 kbit/s~12 Mbit/s 之间选择各种传输速率。

6) **传输距离**：总线的最大传输距离取决于传输速率，范围为 100~1200 m。

对应关系如表 3-2 所示，若有中继器距离可延长到 10 km。

表 3-2 传输速率所对应的最大允许段长度

| 波特率/(kbit/s) | 9.6  | 19.2 | 93.75 | 187.5 | 500 | 1500 | 12000 |
|--------------|------|------|-------|-------|-----|------|-------|
| 段长度/m        | 1200 | 1200 | 1200  | 1000  | 400 | 200  | 100   |

## 2. RS-485 的数据传输过程

RS-485 传输的数据位格式，如图 3-7 所示。

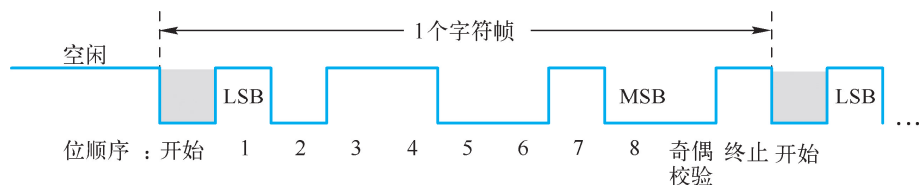


图 3-7 RS-485 传输的数据位格式

数据的发送采用 NRZ 编码方式，1 个字符帧为 11 位。每个 8 位二进制字节按最小的有效位（Least Significant Bit, LSB）先发送，最高的有效位（Most Significant Bit, MSB）最后被发送的顺序传输；每个 8 位二进制数都补充 3 位，即开始、奇偶校验和终止位。用高电位表示“1”，零电位表示“0”；表示“1”的高电位脉冲中途不归零。

站与站数据线的连接方式如图 3-8a 所示，两根 PROFIBUS 数据线也被称为 A 导线和 B 导线，A 导线对应于 RxD/TxD-N 信号，B 导线对应于 RxD/TxD-P 信号。总线终端电阻的连接结构如图 3-8b 所示，包括一个相对于 DGND 数据基准电压的下拉电阻和一个相对于输入正电压 VP 的上拉电阻；当总线上没有发送数据时，即在两个报文之间总线处于空闲状态时，这两个电阻也能确保在总线上有一个确定的空闲电位。

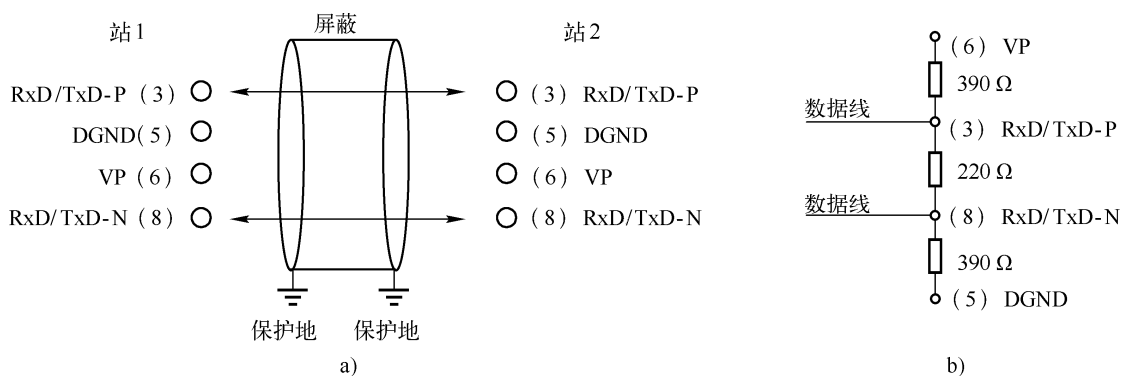


图 3-8 总线的连接

a) 站与站数据线的连接方式 b) A 导线电缆总线终端电阻的连接结构

在数据传输期间，二进制“1”对应于 RxD/TxD-P 线上的正电位，而在 RxD/TxD-N 线上则相反；各报文间的空闲状态对应于二进制“1”信号，如图 3-9 所示。

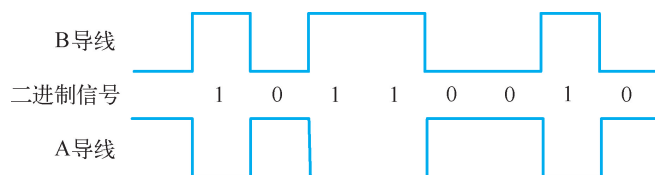


图 3-9 A/B 导线的电位

RS-485 总线的连接结构如图 3-10 所示。根据 EIA RS-485 标准，在数据线 A 和 B 的两端均要连接总线终端器，几乎在所有标准的 PROFIBUS 总线连接器上都组合了所需要的总线终端器，可以由跳接器或开关来启动。

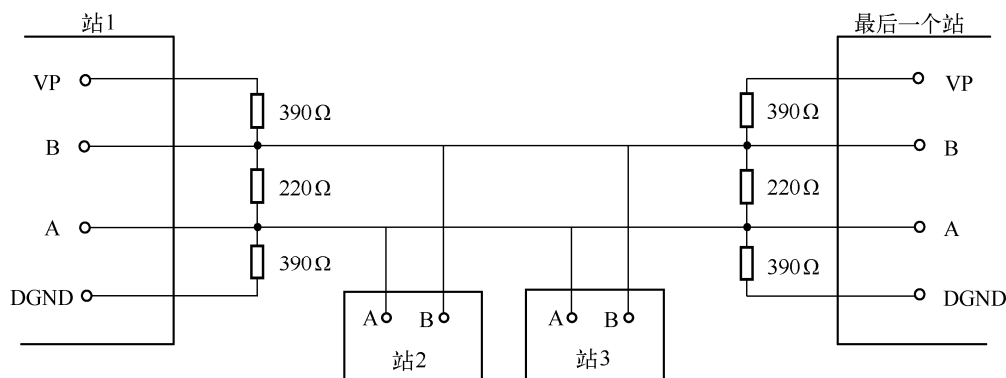


图 3-10 RS-485 总线的连接结构

### 3.2.2 光纤传输技术

在电磁干扰很大的环境或需要覆盖很远的传输距离的网络应用中，可使用光纤传输技术。光纤是一种采用玻璃作为波导，以光的形式将信息从一端传送到另一端的技术。光纤电缆对电磁干扰不敏感并能保证总线上站与站的电气隔离，允许 PROFIBUS 系统站之间的最远距离为 15 km。

现在的低损耗玻璃光纤相对于早期发展的传输介质，几乎不受带宽限制且传输距离远、衰减小。点到的光学传输系统由 3 个基本部分构成：产生光信号的**光发送机**、携带光信号的**光缆**和接收光信号的**光接收机**。

许多厂商提供专用总线插头可将 RS-485 信号转换成光纤信号，或者将光纤信号转换成 RS-485 信号，这使得在同一系统中，可同时使用 RS-485 传输技术和光纤传输技术。为了使光纤导体与总线站连接，可以采用光纤链接模块（Optical Link Module, OLM）、光链路插头（Optical Link Plug, OLP）、集成的光缆和光纤总线终端（Optical Bus Terminal, OBT）等连接技术。

### 3.2.3 IEC 1158-2 传输技术

#### 1. IEC 1158-2 传输技术的特点

IEC 1158-2 传输技术能满足化工、石油等工业对环境的要求，可保证本质安全性和现场设备通过总线供电。这是一种位同步协议，可进行无电流的连续传输，通常称为 H1，采用曼彻斯特编码，能进行本质安全及非本质安全操作；每段只有一个电源作为供电装置，当站收发信息时，不向总线供电。具体特性如下。

- 1) 数据传输：数字式、位同步、曼彻斯特编码。
- 2) 传输速率：通信速率为 31.25 kbit/s，与系统结构和总线长度无关。
- 3) 数据可靠性：前同步信号，采用起始和终止限定符，以避免误差。
- 4) 传输介质：可以采用屏蔽双绞线电缆，也可以采用非屏蔽式双绞线电缆。

- 5) 远程电源供电：为可选附件，可通过数据总线供电。
- 6) 防爆型：能进行本质安全及非本质安全操作。
- 7) 站点数：每段最多有 32 个站点，使用中继器最多可达到 127 个站点。
- 8) 拓扑结构：采用总线型、树形或混合型网络拓扑结构。

## 2. PA 总线结构

PA 总线电缆的终端各有一个无源 RC 线路终端器，如图 3-11 所示。一个 PA 总线上最多可连接 32 个站点，总线的最大长度取决于电源、传输介质的类型和总线站点的电流消耗。

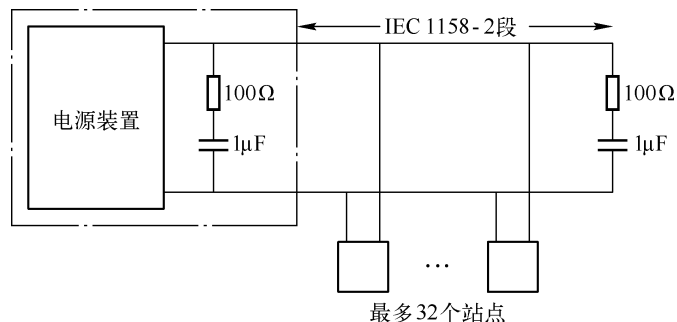


图 3-11 PA 总线的结构

## 3.3 PROFIBUS-DP 控制系统

### 3.3.1 PROFIBUS-DP 设备

PROFIBUS 网络的硬件由主站、从站、网络部件和网络工具等组成。主、从站为控制系统设备；网络部件包括通信介质（例如电缆、光缆等）、总线连接器（例如中继器、RS-485 总线连接器等），以及用于连接串行通信、以太网、执行器/传感器接口（Actuator Sensor Interface, AS-I）、电气安装总线（Electrical Installation Bus, EIB）等网络系统的网络转换器；网络工具包括 PROFIBUS 网络配置、诊断的软件与硬件，用于网络的安装与调试。

PROFIBUS-DP 控制系统使用的典型设备如图 3-12 所示。

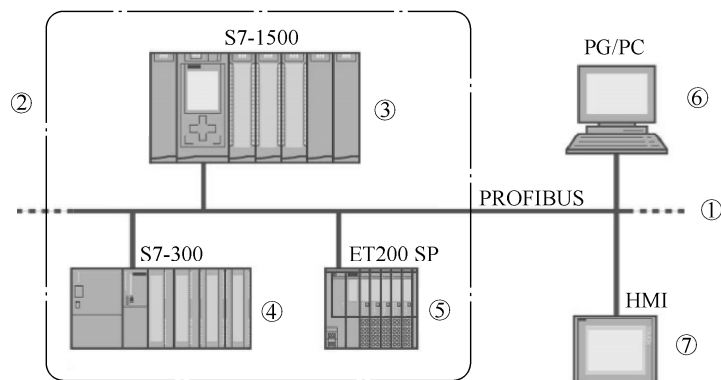


图 3-12 PROFIBUS-DP 控制系统使用的典型设备

设备性能说明如下。

① PROFIBUS：网络架构。

② DP 主站系统：单主站系统。

③ DP 主站：用于对连接的 DP 从站进行寻址的设备。

该类设备属于 1 类主站。1 类主站（DPM1）是中央控制器，可完成总线通信控制、管理及周期性数据访问。无论 PROFIBUS 的网络采用何种结构，1 类主站是系统必需的。比较典型的 DPM1 有 PLC、PC、支持主站功能的各种通信处理器模块等设备。

④ 智能从站：智能 DP 从站。

⑤ DP 从站：分配给 DP 主站的分布式现场设备。

从站是对数据和控制信号进行输入/输出的设备。从站在主站的控制下，进行现场输入信号的采集与控制信号的输出。作为从站的设备可以是 PLC 一类的控制器，也可以是不具有程序存储和程序执行功能的分散式 I/O 设备，还可以是像 SITRANS（现场仪表）和 MicroMaster（变频器）这样的具有总线接口的智能现场设备。

⑥ PG/PC、⑦ HMI：用于系统调试、诊断和监控的设备。

该类设备属于 2 类主站。2 类主站（DPM2）可完成非周期性数据访问，如数据读写、系统配置、故障诊断及管理组态数据等，它可以与 1 类主站进行通信，也可以与从站进行输入/输出数据的通信，并为从站分配新的地址。DPM2 主要是在工程设计、系统组态或操作设备时使用，比较典型的 DPM2 有编程设备、触摸屏、操作面板等设备。

### 3.3.2 PROFIBUS-DP 的 IO 通信

IO 通信就是对分布式 IO 的输入/输出进行读写操作，如图 3-13 所示。IO 通信可以通过设备本身集成的 DP 接口完成，也可以通过通信模块（CM）或带有集成 DP 接口的接口模块（IM）来完成。

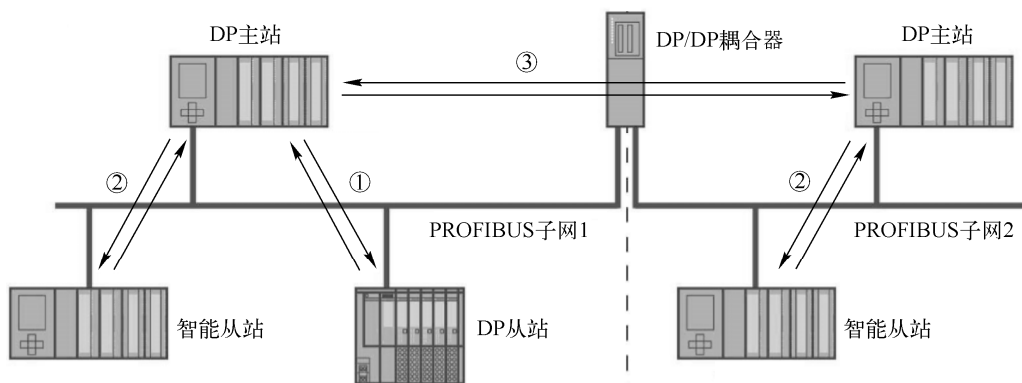


图 3-13 PROFIBUS-DP 的 IO 通信

① DP 主站与 DP 从站之间的通信：DP 主站与 DP 从站之间的通信按照主从方式进行通信。DP 主站依次查询主站系统中的 DP 从站，接收 DP 从站的数据，然后将输出数据回传给 DP 从站。

② DP 主站与智能从站间的通信：DP 主站不能访问智能从站的 I/O 模块，但可以访问所组态的地址区域（传输区域）。这些区域可位于智能从站 CPU 的过程映像的内部或外部；若将过程映像的某些部分用作传输区域，则不能将这些区域用于实际 I/O 模块的物理地址；



数据传输是通过使用该过程映像的加载和传输操作或通过直接访问进行的。

③ **DP 主站与 DP 主站间的通信**：DP 主站之间的通信需要增加 DP/DP 耦合器，以循环传输固定数量的数据。各 DP 主站相互访问位于 CPU 的过程映像的内部或外部的已组态的地址区域（传输区域）。若将过程映像的某些部分用作传输区域，则不能将这些区域用于实际 I/O 模块的物理地址；数据传输也是通过使用该过程映像的加载和传输操作或通过直接访问进行的。

### 3.3.3 GSD 文件

#### 1. GSD 文件简介

由于 PROFIBUS-DP 是一种通信标准，因此符合 PROFIBUS-DP 规约的第三方设备也可以加入 PROFIBUS 网络。为了将不同厂商生产的 PROFIBUS 产品集成在一起，生产厂商必须为其产品提供电子 GSD 文件。**GSD（General Station Description）文件是对 PROFIBUS-DP 设备性能的描述**，例如对设备的波特率、信息长度、诊断信息等参数进行详细说明，通常以 \*.GSD 或 \*.GSE 文件名出现，将 GSD 文件导入到编程软件中就可以在硬件配置界面的目录中找到这个设备并组态通信接口。

#### 2. GSD 文件的组成

GSD 文件包含用于通信通用的和设备专用的规范，其文件结构可以分为以下 3 个部分。

1) **一般规范**。这部分包括制造商的信息、设备的名称、硬件和软件的版本状况、所支持的传输速率、可能的监视时间间隔以及在总线连接器上的信号分配等。

2) **与 DP 主站有关的规范**。这部分包含所有与主站有关的参数，如最大可连接的从站个数、上装和下载选项等。这部分内容不能用于从站设备。

3) **与 DP 从站有关的规范**。这部分包括与从站有关的信息，如输入/输出通道的数量和类型、中断测试的规范、输入/输出数据一致性的信息等。

#### 3. GSD 文件格式

GSD 是可读的 ASCII 文本文件，可以用任何一种 ASCII 编辑器进行编辑（如记事本、UltraEdit 等），也可使用 PROFIBUS 用户组织提供的编辑程序（GSDEdit）编辑。GSD 文件由若干行组成，每行都用一个关键字开头，包括关键字及参数（无符号数或字符串）两部分。借助于关键字，组态工具从 GSD 文件中读取用于设备组态的设备标识、可调整的参数、相应的数据类型和所允许的界限值。GSD 文件中的关键字有些是强制性的，例如 VendorName；有些关键字是可选的，例如 SyncMode Supp。GSD 代替了传统的手册，并在组态期间支持对输入错误及数据一致性的自动检查。

某一通信模块的 GSD 文本如下。

|                       |                        |
|-----------------------|------------------------|
| #PROFIBUS DP          | ;DP 设备的 GSD 文件均以此关键词存在 |
| GSD Revision=1        | ;GSD 文件版本              |
| VendorName="Meglev"   | ;设备制造商                 |
| Model Name="DP Slave" | ;从站模块                  |
| Revision="Version 01" | ;产品名称,产品版本             |
| :                     |                        |
| EndModule             |                        |



通过将 GSD 文件读取到组态程序中，用户可以获得最适合使用的设备专用通信特性。为了支持设备商，PROFIBUS 网站上有专用的 GSD 编辑/检查程序可供下载，便于用户创建和检查 GSD 文件，也有专用的 GSD 文件库供相关设备的用户下载使用。

## 3.4 基于智能从站（PLC）的 PROFIBUS-DP 通信实现

### 3.4.1 控制系统硬件配置

本例采用 PROFIBUS-DP 通信方式，完成两台 S7-300 PLC 之间的信息交换和控制功能。具体要求如下。

- 1) 主站输入信号控制从站侧电动机的运行和停止。
- 2) 从站输入信号控制主站侧电动机的运行和停止。
- 3) 电机按照运行 3 s、停止 3 s 的周期工作，如此循环。

根据系统控制要求，系统配置如下：CPU313C-2DP PLC 两台；PROFIBUS-DP 通信电缆一根；PC 一台；PC/Adapter 编程电缆一根；编程软件为 TIA PORTAL V15 professional（可参见附录 A）。

S7-300 PLC 基于模块化结构设计，适用于中小型控制系统。CPU313C-2DP PLC 是紧凑型 CPU，适合安装在分布式结构中，集成的数字量 I/O 可直接与过程系统相连接，PROFIBUS-DP 接口允许连接独立的 I/O 单元，既可以作为主站，也可以作为智能从站，用来建立高速、易用的分布式自动化系统。

系统结构如图 3-14 所示。



图 3-14 系统结构图

主站与从站之间数据传送变量地址分配如下。

- 1) 主站输入/输出（I/O）地址分别设置为：IB124、IB125，QB124、QB125。
- 2) 从站输入/输出（I/O）地址分别设置为：IB124、IB125，QB124、QB125。
- 3) 主站与从站的站号、数据交互变量地址及对应关系设置如图 3-15 所示。

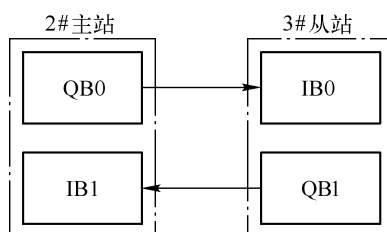


图 3-15 主站与从站之间的数据传送图

### 3.4.2 硬件组态

## 1. 有关硬件组态

运行 PROFIBUS 系统之前，需要先对系统及各站点进行硬件配置和相关参数的设置，即对系统进行硬件组态，这项工作可以由编程软件 TIA PORTAL 来实现。硬件组态是将系统实际使用的 CPU、信号模块（SM）、通信模块（CM）等配置到对应的插槽上，并对各个硬件进行参数设置，这项操作对于控制系统的正常运行非常重要。它的主要功能如下。

- 1) 将配置好的信息下载到 CPU 中，使 CPU 按照配置的参数执行。
- 2) 将 I/O 模块的物理地址进行分配，映射为逻辑地址，便于程序块调用。
- 3) CPU 将会比较模块的配置信息与实际安装的模块是否匹配，如 I/O 模块、AI/AQ 模块的安装位置、测量类型、型号等；如不匹配，CPU 将报警并将故障信息存储到诊断缓存区，方便用户进行相应的修改。
- 4) CPU 将根据配置信息对模块进行实时监控，若模块有故障，CPU 将报警并将故障信息存储到诊断缓存区。
- 5) 一些智能模块 [如通信的 CP/CM 模块、工艺模块 (TM) 等] 的配置信息存储到 CPU 中，若出现模块故障，可直接更换，不需要重新下载配置信息。
- 6) 第三方设备集成及 GSD 文件安装与使用。

当 PROFIBUS 系统中需要使用第三方设备时，应该得到设备厂商提供的 GSD 文件。将 GSD 文件复制到软件的指定目录下，即可通过软件在友好的界面指导下完成第三方产品在系统中的配置及参数设置等工作。

例如，S7-200 PLC 不支持 DP 通信协议，自身也不带 PROFIBUS-DP 接口，但可以通过添加通信扩展模块 EM277，将 S7-200 作为从站连接到 PROFIBUS-DP 网络中，导入路径为：菜单栏的“选项”→“管理通用站描述文件(GSD)(D)”。图 3-16 为 EM277 模块的 GSD 文件导入路径界面，当 GSD 文件导入后，单击“安装”按钮，出现如图 3-17 所示的安装过程界面；安装完成后，可以在 TIA PORTAL 软件的硬件目录中找到相应模块的配置文件，并可进行 S7-200 PLC 通信接口的硬件组态，如图 3-18 所示。

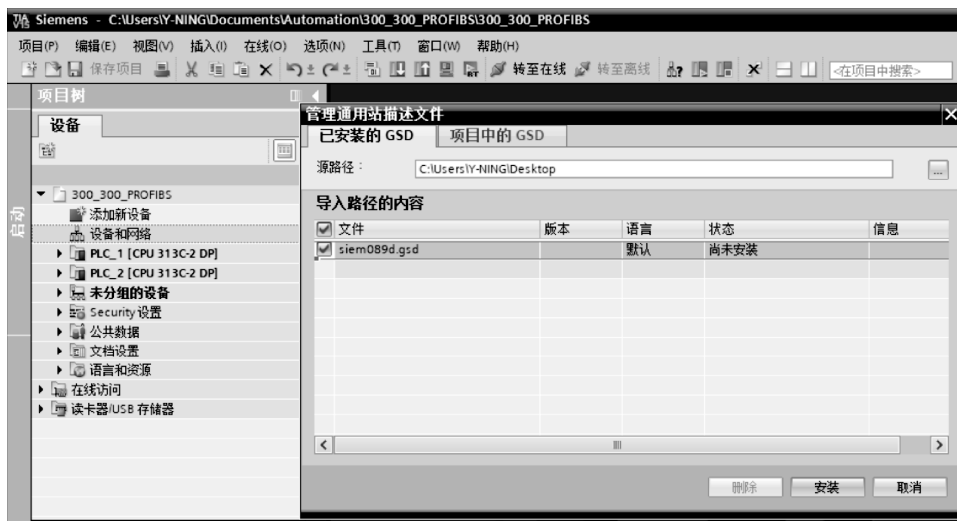


图 3-16 GSD 文件导入



图 3-17 GSD 文件安装



图 3-18 EM277 模块的选用

## 2. 新建项目

在 TIA PORTAL 软件工程界面的“Portal 视图”和“项目视图”下，均可以组态新项目。

单击 PORTAL V15 快捷键，进入“Portal 视图”界面。如图 3-19 所示，在“Portal 视图”界面下，单击“创建新项目”选项，创建新项目“300\_300\_PROFIBUS”；然后单击“创建”按钮，生成新项目，如图 3-20 所示。



图 3-19 项目的建立



图 3-20 新项目的“Portal 视图”界面

“Portal 视图”是以向导的方式来组态新项目，“项目视图”则是硬件组态和编程的主视窗。单击图 3-20 中左下角的“项目视图”，进入如图 3-21 所示的“项目视图”界面。

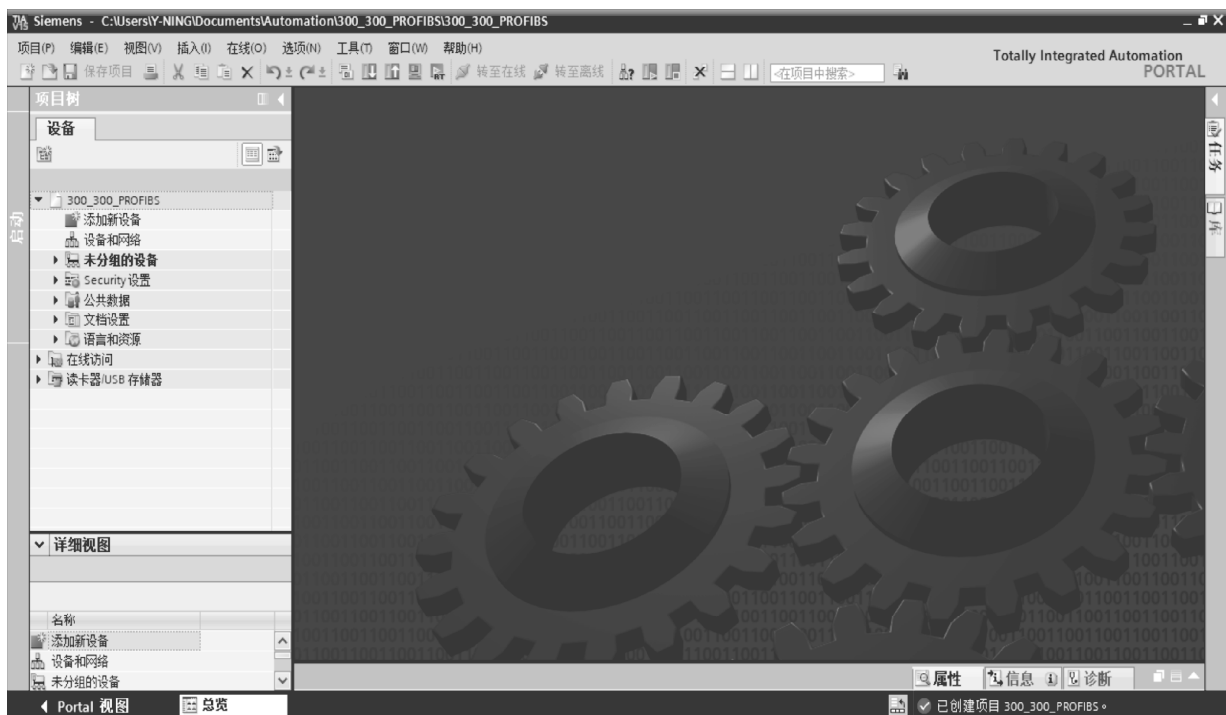


图 3-21 “项目视图”界面

### 3. 添加新设备

如图 3-22 所示,选中并双击项目树中的“添加新设备”选项,输入“设备名称”,选择 PLC 类型、订货号、版本号,单击“确定”按钮,弹出如图 3-23 所示界面。



图 3-22 设备选择

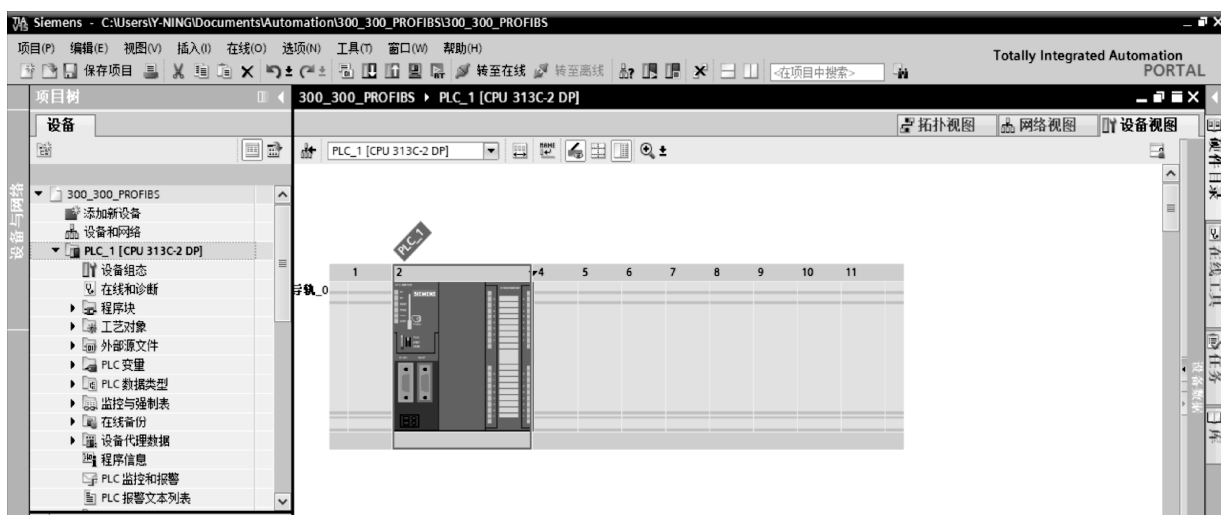


图 3-23 设备视图

### 4. I/O 地址分配

对设备进行输入/输出地址分配。如图 3-24 所示,在“设备视图”中选中 PLC\_1 模块,进入“属性”→“常规”→“DI 16/DO16”→“输入”→“I/O 地址”界面,设定 PLC 的输入/输出通道地址。默认输入/输出起始地址为 124,可以在 0~1022 范围内更改;本例 PLC\_1 模块分配的输入/输出地址为默认值。

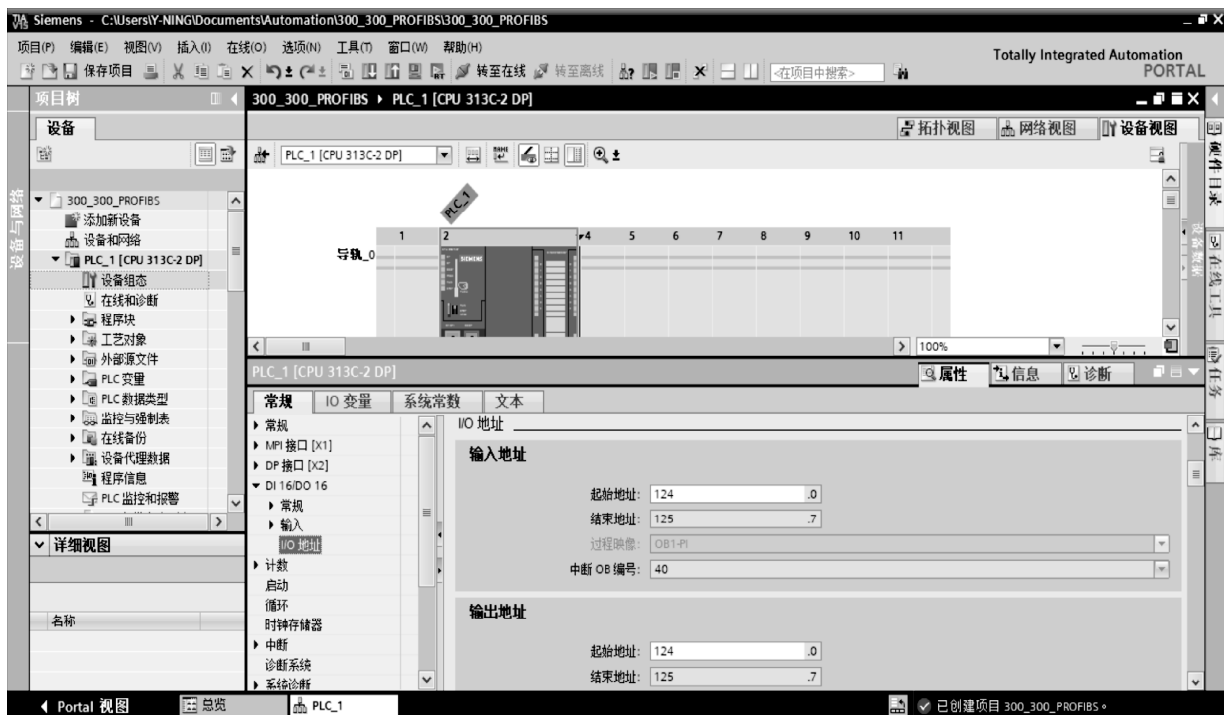


图 3-24 PLC\_1 输入/输出地址分配

同理，添加第二台设备，设备名称为 PLC\_2。本例分配输入/输出地址为默认值，即输入地址为 IB124、IB125，输出地址为 QB124、QB125。项目的网络视图如图 3-25 所示。

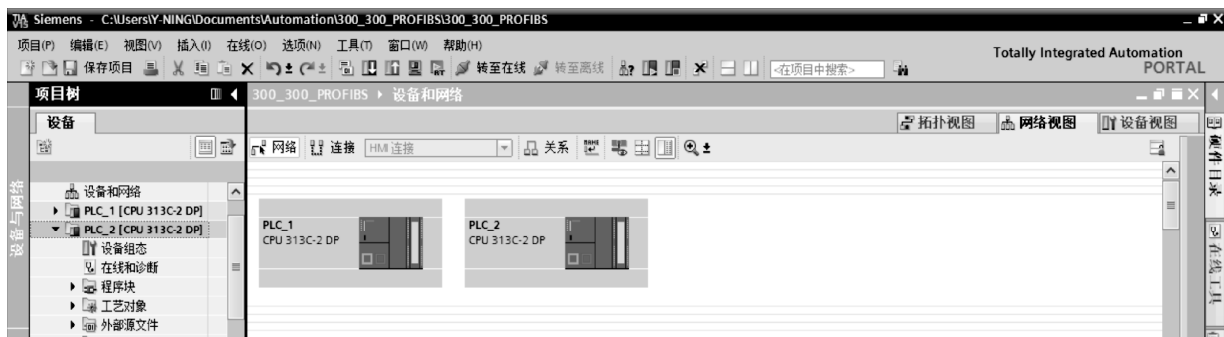


图 3-25 网络视图

### 3.4.3 通信接口参数设置

#### 1. 主站接口参数设置

1) 在“设备视图”中，双击 PLC\_1 设备的 PROFIBUS DP 接口，弹出通信接口配置界面，如图 3-26 所示。

2) 单击“添加新子网”按钮，自动生成 DP 总线子网“PROFIBUS\_1”，网络地址为 2，传输速率为 1.5 Mbit/s，如图 3-27 所示，本例选择默认值。

3) 在“DP 接口\_1”的“常规”选项卡，选择“操作模式”，如图 3-28 所示。默认选项为“主站”。

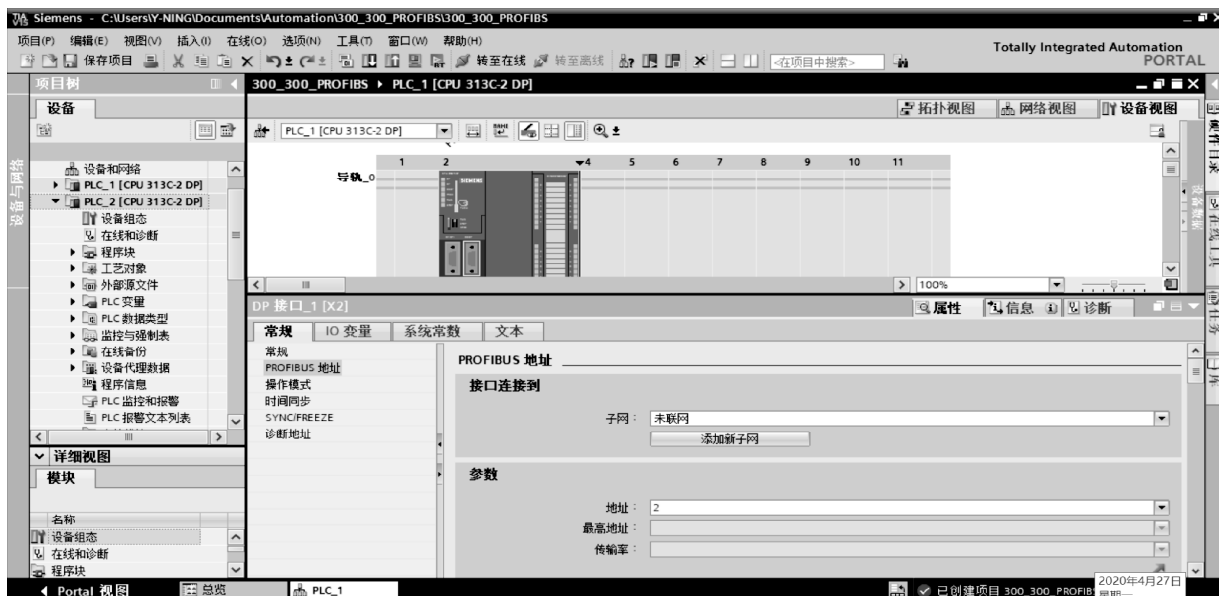


图 3-26 通信接口配置界面

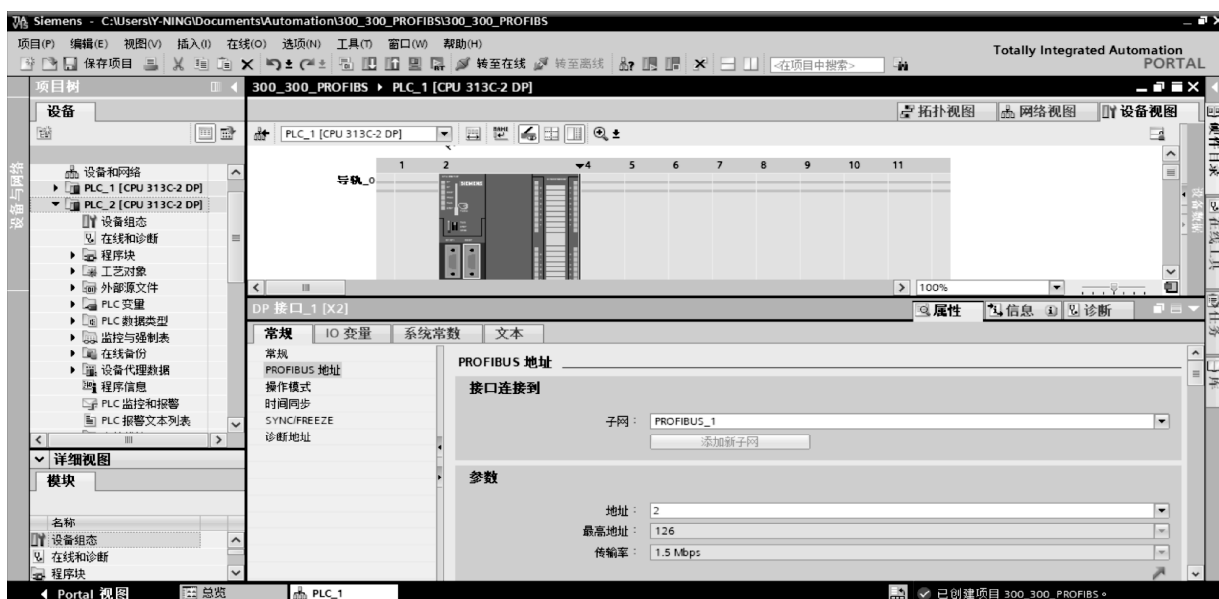


图 3-27 配置 PLC\_1 接口参数



图 3-28 PLC\_1 操作模式选择

## 2. 智能从站接口参数设置

1) 同样，在“设备视图”中双击 PLC\_2 设备的 PROFIBUS DP 接口，选择子网“PROFIBUS\_1”、更改网络地址为 3，完成接口通信参数设置，如图 3-29 所示。

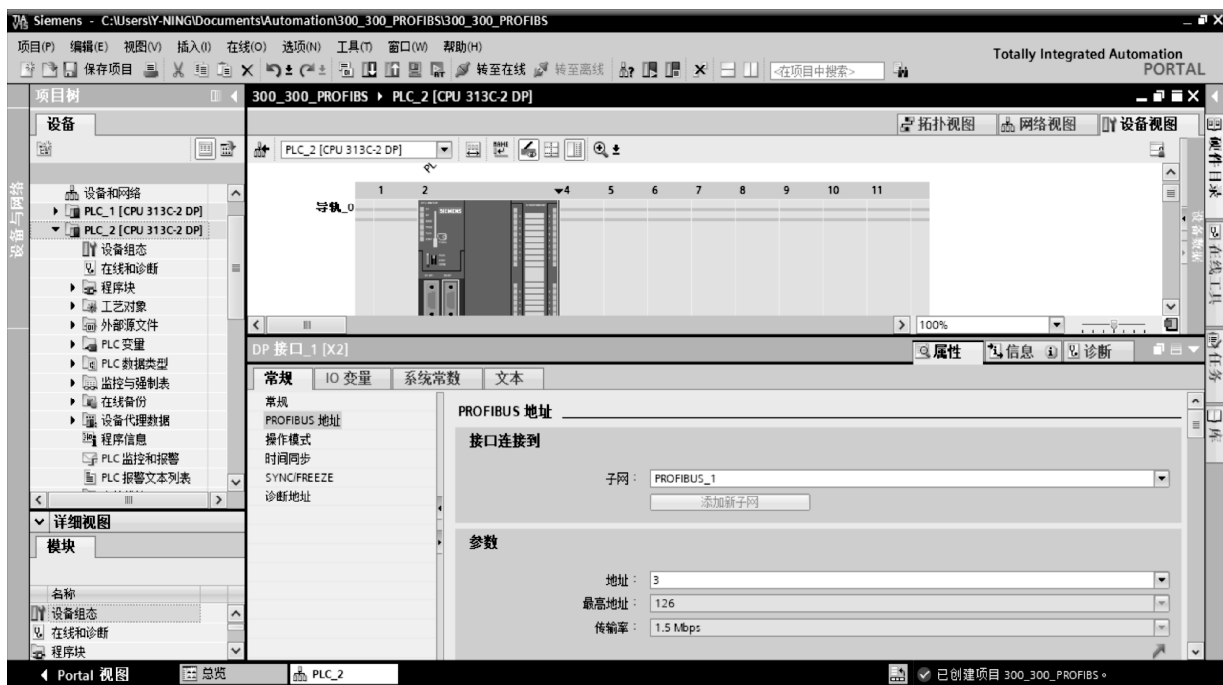


图 3-29 配置 PLC\_2 接口参数

2) 进入“操作模式”，将 PLC\_2 设备更改为“从站”模式，并配置该从站被分配的 DP 主站，勾选“测试、运行和路由”复选框，如图 3-30 所示。

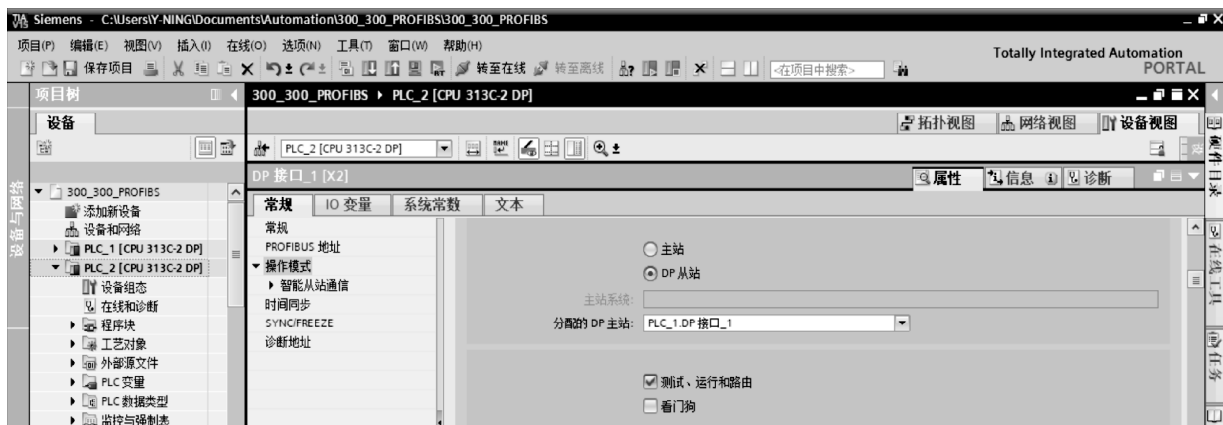


图 3-30 PLC\_2 操作模式选择

3) 设置“操作模式”下的“智能从站通信”参数。考虑主站、从站通信变量地址对应关系，设置通信变量传输区域，界面如图 3-31 所示。

- ① 通信方向总是从输出 Q 区到输入 I 区，单击通信方向箭头，可以设置通信的地址区。
- ② “单位”可以选择“字节”，也可以选择“字”。
- ③ “一致性”可以选择“单元”，也可以选择“总长度”。



图 3-31 设置通信变量传输区域

所谓数据的一致性是指在 PROFIBUS-DP 数据传输时，数据的各个部分在传输时不会被割裂，保证同时更新，以免数据传输错误。选择“单元”，表示通信数据中每字节都是独立的单元；选择“总长度”，表示通信数据是一个数组，通信数据在同一数据包中。

### 3. 项目网络视图

1) PROFIBUS 网络配置完成后，单击“网络视图”，网络连接界面如图 3-32 所示，单击“显示地址”，可查看 PROFIBUS 地址分配是否正确。

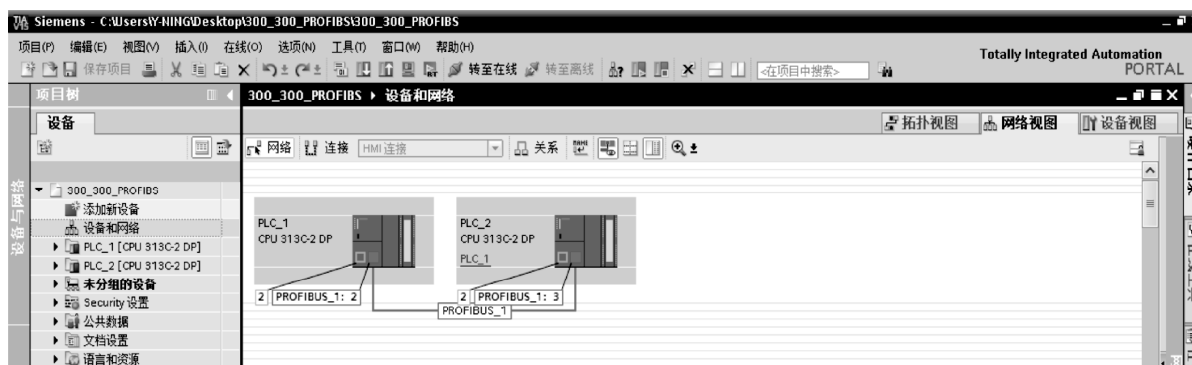


图 3-32 项目网络视图

2) 保存并编译 PLC\_1 硬件组态，并将硬件组态下载至 PLC\_1 对应的 PLC 中；保存并编译 PLC\_2 硬件组态，并将硬件组态下载至 PLC\_2 对应的 PLC 中。

### 3.4.4 程序设计与系统调试

#### 1. PLC 的 I/O 地址分配

主站、从站 PLC 的 I/O 地址分配如表 3-3 和表 3-4 所示。

表 3-3 主站 PLC 的 I/O 地址分配

| PLC 的 I/O 地址 | 连接的外部设备   | 在控制系统中的作用   |
|--------------|-----------|-------------|
| I125. 0      | 按钮 SB1    | 从站电动机起动按钮   |
| I125. 1      | 按钮 SB2    | 从站电动机停止按钮   |
| Q125. 1      | 接触器线圈 KM1 | 主站电动机 M1 工作 |



表 3-4 从站 PLC 的 I/O 地址分配

| PLC 的 I/O 地址 | 连接的外部设备   | 在控制系统中的作用   |
|--------------|-----------|-------------|
| I125.0       | 按钮 SB3    | 主站电动机起动按钮   |
| I125.1       | 按钮 SB4    | 主站电动机停止按钮   |
| Q125.0       | 接触器线圈 KM2 | 从站电动机 M2 工作 |

2. 控制功能的实现

根据控制要求、PLC 的 I/O 地址分配及通信传输区域设置，分别在 PLC 的 Main（OB1）中编写程序，主站程序编写如图 3-33a 所示，从站程序编写如图 3-33b 所示，并将主站、从站程序块分别下载至对应的 PLC 中。

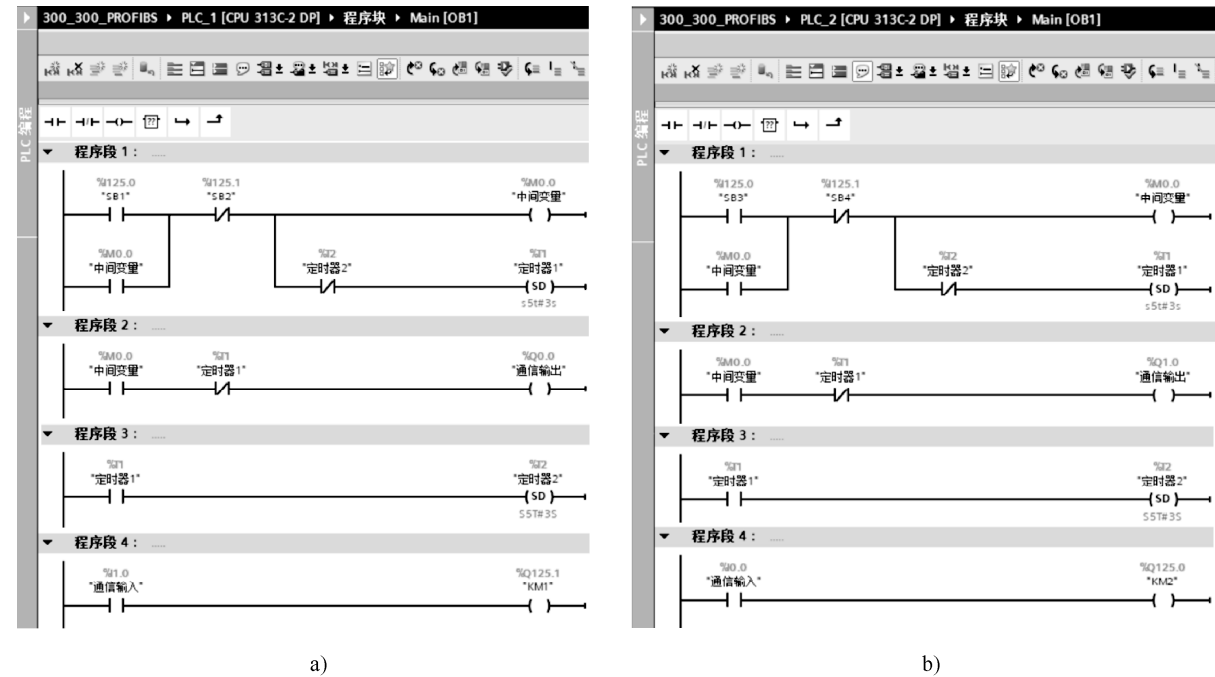


图 3-33 主站和从站程序的编写

a) 主站程序 b) 从站程序

3. 系统联调及注意事项

为保证通信正常运行，可在主站、从站中分别创建 OB82（诊断中断）、OB86（机架故障或分布 I/O 故障）、OB87（通信故障处理）及 OB122（I/O 访问错误）等组织块。

当系统出现故障时，CPU 会进入相应的中断（寻找 OB）处理，如果找不到相应的 OB，系统将会停机，因此建立相应故障的 OB 块可以防止 CPU 停机；OB 块可以是空程序，也可以根据项目的具体使用情况编写执行程序。

系统调试前，需要保证每个 PLC 的硬件组态、程序块都下载至相应的 PLC 中，且外部接线正确，如图 3-34 所示。

系统主站运行的在线监控如图 3-35 所示，变量“通信输入（%I1.0）”为主站接收从站的控制信号；主站电动机状态控制变量 KM1 程序的在线监控如图 3-36 所示，其中实线（绿色）为电动机运行状态，虚线（蓝色）为电动机停止状态。



图 3-34 从站设备项目下载



图 3-35 主站变量在线监控

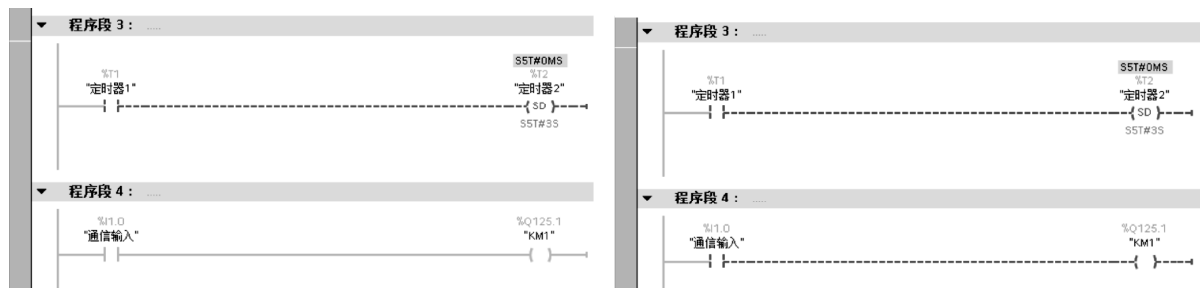


图 3-36 主站电动机控制 KM1 状态

### 3.5 基于 DP 从站（变频器）的 PROFIBUS-DP 通信实现

#### 3.5.1 控制系统硬件介绍

##### 1. 控制系统硬件配置

本例采用 PROFIBUS-DP 通信方式，实现 S7-300 PLC 在线获得 MM420 变频器的运动状态，并且可以在线修改变频器的运行状态和转速。

根据系统控制要求，系统配置如下：CPU314C-2DP PLC 1 台，订货号：6ES7 314-6CH04-0AB0 V3.3；电源模块 PS 307 2A 1 块，订货号：307-1BA01-0AA0；变频器 MM420 DP 模块，订货号：6SE6 400-1PB00-0AA0；PROFIBUS-DP 通信电缆 1 根；PC 1 台；PC/

Adapter 编程电缆 1 根；编程软件为 TIA PORTAL V15 professional。

系统结构如图 3-37 所示。



图 3-37 系统结构图

## 2. MM420 变频器简介

为了连接进入 PROFIBUS-DP 网络，变频器必须采用 PROFIBUS 模板，这一模板安装在变频器的正面，通过 RS-485 串行接口与变频器进行通信。

选择带 DP 接口的 MM420 变频器作为从站，相关参数如下。

- 1) 变频器货号：6SE6 420-2UC11-2AA1；
- 2) 输入电压范围：200~240 V/(+10%~-10%)；
- 3) 输出电压范围：0~输入电压，三相交流；
- 4) 输出频率范围：0~650 Hz；
- 5) 适配电动机功率：0.12 kW。

## 3. PROFIBUS 总线系统硬件连接及参数设置

1) 正确连接主站和变频器之间的总线电缆，包括必要的终端电阻和各段网络。

2) 总线电缆必须是屏蔽电缆，其屏蔽层必须与电缆插头/插座的外壳相连。

3) 变频器的从站地址（参数 P0918）必须正确设置，使它与 PROFIBUS 主站配置的从站地址相一致。变频器常用操作模式有 3 种。

① 基本操作面板（BOP）操作。一般先设定 P0010 = 30，P970 = 1，把其他参数复位，然后设定 P0010 = 0，P0700 = 1，P1000 = 1。

② 外部（通过端子排）输入控制。一般先设定 P0010 = 30，P970 = 1，把其他参数复位，然后设定 P0010 = 0，P0700 = 2，P1000 = 2。

③ PROFIBUS 总线控制。一般先设定 P0010 = 30，P970 = 1，把其他参数复位，然后设定 P0010 = 0，P0700 = 6，P1000 = 6。

本例中将变频器设置为 PROFIBUS 总线控制状态。

也可以在变频器的通信板（CB）上完成，通信板（CB）上有一排拨钮用于设置地址，如图 3-38 所示，每个拨钮对应于“8-4-2-1”码<sup>①</sup>的数据，当所有的拨钮处于“ON”状态时，对应的数据相加的和就是站地址。例如，如果设置变频器站地址为 3，则将 1、2 位置的拨钮置在“ON”的状态；拨钮开关为“0”时，P0918 指定的地址有效，不为“0”时，拨钮的设定值优先。

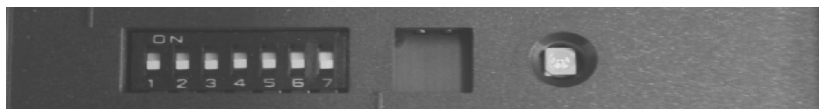


图 3-38 通信板上的拨钮开关

变频器从站地址必须和 PORTAL 软件中硬件组态的地址保持一致，否则不能通信。

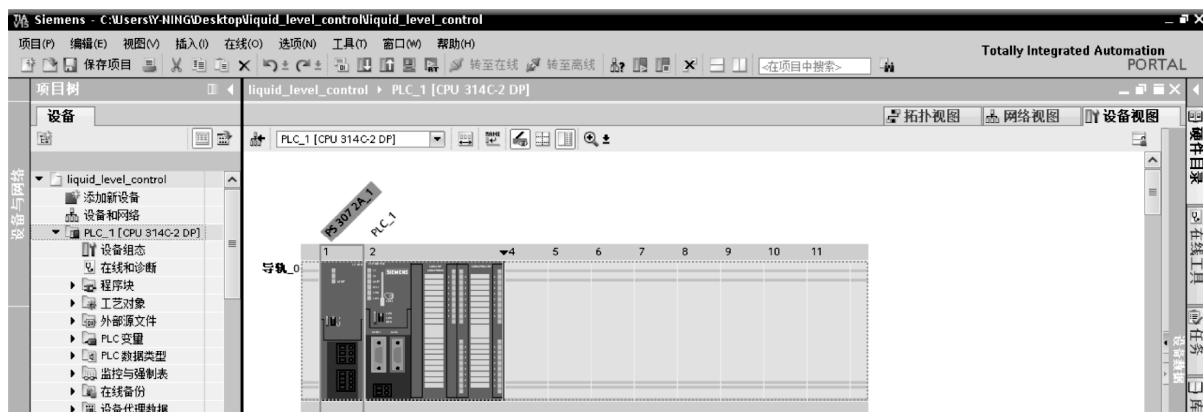
① 又称为 BCD 码，是十进制代码中最常用的一种。

### 3.5.2 硬件组态及网络连接

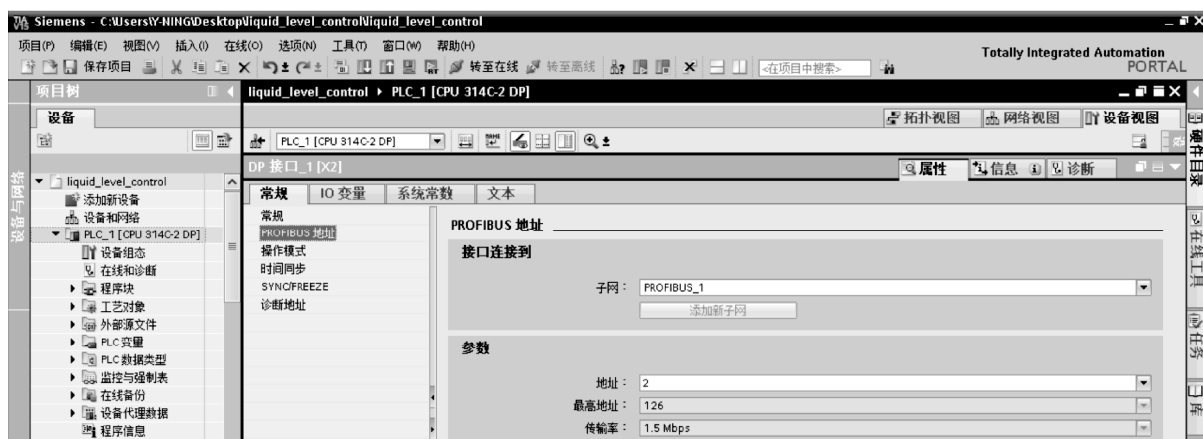
#### 1. 主站硬件组态

打开 TIA Portal 编程软件，新建项目，添加新设备“PLC\_1”，如图 3-39a 所示，单击 PROFIBUS-DP 接口，设置该站点的网络参数，如图 3-39b、c 所示。

3-1 系统硬件组态



a)



b)



c)

图 3-39 主站硬件组态

a) 新建 PLC\_1 站点 b) 设置 PLC\_1 站点 DP 接口的 PROFIBUS 地址 c) 设置 PLC\_1 站点 DP 接口的操作模式

## 2. MM420 从站的组态

1) 在“网络视图”界面，选择“硬件目录”下的“其他现场设备”→“PROFIBUS DP”→“驱动器”→“SIMOVERT”→“MICROMASTER 4”，如图 3-40 所示。

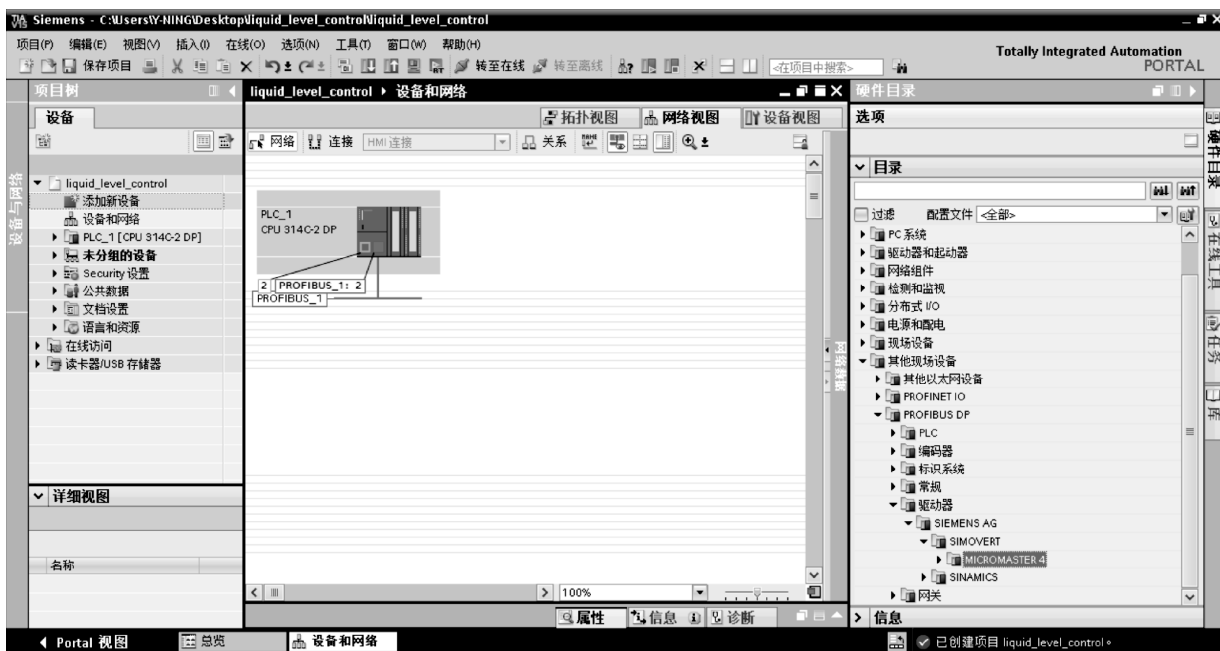


图 3-40 MICROMASTER 4 在“硬件目录”中的位置

2) 单击“前端模块”，将模块拖拽到“网络视图”界面，如图 3-41 所示。单击“Slave\_1”的“未分配”位置，选择“选择主站”并单击，出现如图 3-42 所示界面。



图 3-41 添加变频器通信接口



图 3-42 主从站的通信连接

3) 选中“变频器”图标并双击，弹出如图 3-43 所示界面。将工作方式“0 PKW, 2PZD (PPO 3)”拖拽到插槽 1 上，进行 MM420 从站配置。该通信报文格式的含义是报文中有 0 个字的 PKW (参数标识值)，有 2 个字的 PZD (过程数据)。由 PKW 和 PZD 组成多种 PPO 形式，可根据设计需要选择合适的形式。

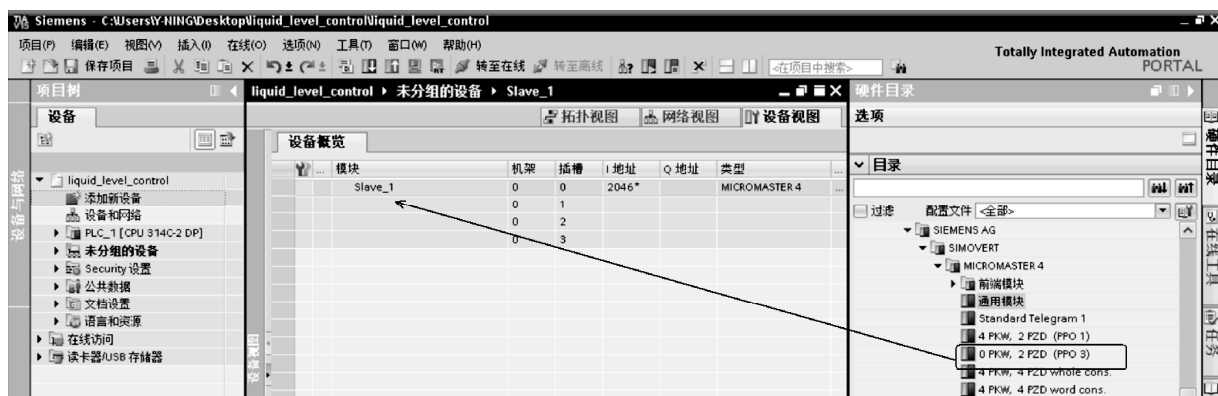


图 3-43 设置 DP 从站工作方式

4) 如图 3-44 所示，将主站读取 MM420 数据的地址设置为 IB290~IB293 (默认值为：IB256~IB259) 中，共 2 个字；将主站向 MM420 写入数据的地址设置为 QB272~275 (默认值为：QB256~QB259)，共 2 个字。最后，编译并保存组态完成的硬件设置。



图 3-44 设置 DP 从站数据通道的地址

### 3. 网络视图

在“网络视图”界面，通过单击“显示地址”查看设备通信地址设置情况，如图 3-45 所示。可见，通过上述操作 DP 从站获得默认地址 3，如需修改变频器地址可通过单击界面上变频器图标接口来修改变频器的地址。

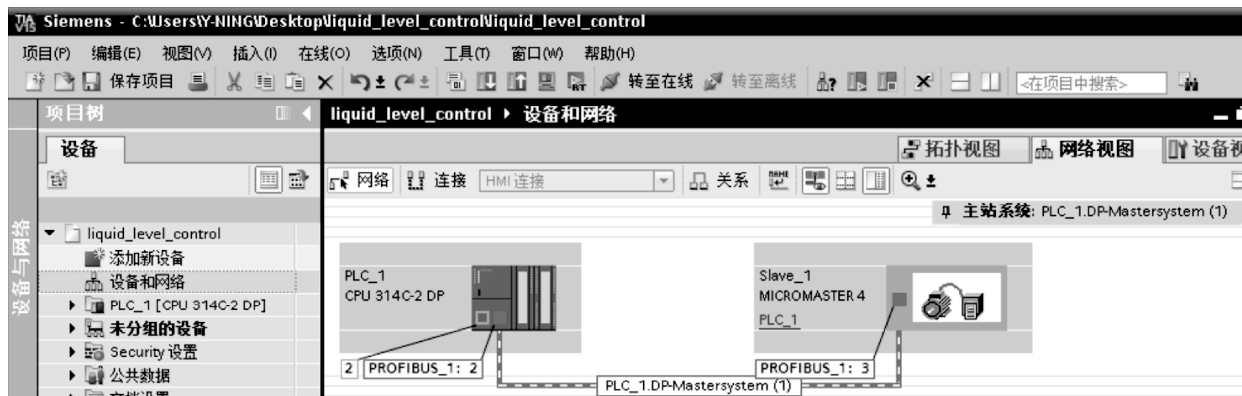


图 3-45 系统网络视图



### 3.5.3 程序设计与系统调试

#### 1. 变频器的控制字和状态字

PKW 用于读写变频器中的某个参数，PZD 是为控制和监测变频器而设计的。如果要控制变频器起停、设定频率等参数，则需要用到 PZD，过程数据一直被传输，具有最高的优先级和最短的间隙，其数据根据传送方向不同而不同：当主站读取变频器的数据时，PZD 区由返回变频器的状态字 ZSW 和实际速度值 HIW 构成；当主站向变频器写入数据时，PZD 区由控制字 STW 和频率设定值 HSW 构成。状态字与控制字含义分别如表 3-5 和表 3-6 所示。



3-2 主站程序编写

表 3-5 状态字含义 (ZSW)

| Bit7   | Bit6     | Bit5    | Bit4      | Bit3      | Bit2   | Bit1     | Bit0      |
|--------|----------|---------|-----------|-----------|--------|----------|-----------|
| 驱动警告激活 | 激活禁止合闸状态 | OFF3 激活 | OFF2 激活   | 驱动故障      | 驱动正在运行 | 驱动就绪等待运行 | 驱动就绪      |
| Bit15  | Bit14    | Bit13   | Bit12     | Bit11     | Bit10  | Bit9     | Bit8      |
| 变频器过载  | 电动机顺时针运行 | 电动机过载   | 电动机保持制动激活 | 电动机最大电流警告 | 达到最大频率 | PZD 控制   | 设定值/实际值偏差 |

表 3-6 控制字含义 (STW)

| Bit7  | Bit6  | Bit5   | Bit4   | Bit3  | Bit2   | Bit1 | Bit0    |
|-------|-------|--------|--------|-------|--------|------|---------|
| 故障确认  | 设定值使能 | RFG 开始 | RFG 使能 | 脉冲使能  | OFF3   | OFF2 | ON/OFF1 |
| Bit15 | Bit14 | Bit13  | Bit12  | Bit11 | Bit10  | Bit9 | Bit8    |
| —     | 电位计降速 | 电位计升速  | —      | 设定值反向 | PLC 控制 | 点动向左 | 点动向右    |

例如：当主站向变频器写入数据 16#047E，表示停止；写入数据 16#047F，表示启动/前进；写入数据 16#0C7F，表示启动/后退。

#### 2. PLC 通信指令

在 PLC 与变频器数据传输过程中，最常用的是通过调用系统功能块实现两者之间的通信，即在 PLC 的 OB1 中调用系统功能 SFC14(DPRD\_DAT)/SFC15(DPWR\_DAT)，完成对 MM420 数据的读写功能。通信指令结构及调用路径如图 3-46 所示。

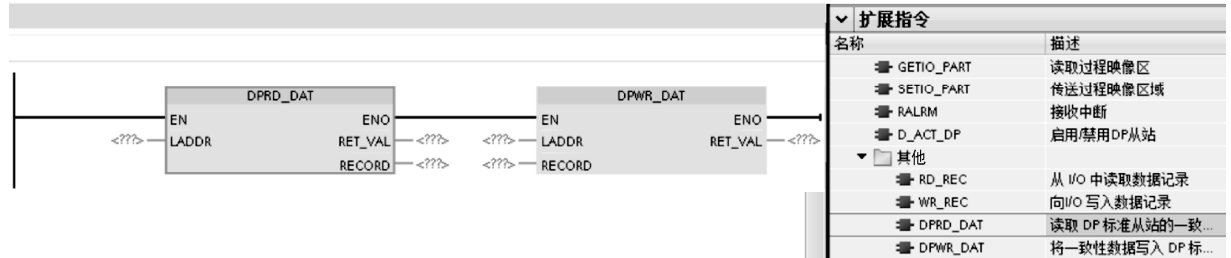


图 3-46 通信指令结构及调用路径

##### (1) DPRD\_DAT 指令

该指令为读取 DP 从站的一致性数据。指令引脚 LADDR (WORD 型) 是待读取数据的智能模块的通信起始地址，且地址必须用十六进制格式指定；本例中组态为 IW290(16#122)；RET\_VAL(INT 型) 用来存放指令执行过程中的返回值，包括错误代码；RECORD(ANY 型)

用于存放读取的目标数据。

### (2) DPWR\_DAT 指令

该指令为将一致性数据写入 DP 从站。指令引脚 LADDR (WORD 型) 是将数据写入智能模块的通信起始地址, 且地址必须用十六进制格式指定; 本例中组态为 QW272(16#110); RECORD(ANY 型) 为写入从站数据的源数据区域; RET\_VAL(INT 型) 用来存放指令执行过程中的返回值, 包括错误代码。

### 3-3 系统调试与运行



### 3. 控制功能的实现

主站 PLC 的 Main[OB1] 程序设计如图 3-47 所示。



图 3-47 主站 PLC 的 Main[OB1] 程序

“状态值和实际速度值”变量为主站从变频器读到的状态字和实际速度值, “控制字和设定频率”变量为主站向从站写入的控制字和频率给定值。图 3-48 为这两个变量在停止、启动及稳定运行时的 3 组数据, 读者可对照表 3-5 自行分析数据含义。

在设定变频器频率时需要注意实际频率与通信变量之间的对应关系 (见表 3-7), 本例将变频器的运行频率设定为 25 Hz (16#2000)。

表 3-7 变频器实际频率与通信变量之间的对应关系

| 频率实际值/Hz | 十六进制对应值 | 十进制对应值 |
|----------|---------|--------|
| 50       | 4000    | 16384  |
| 37.5     | 3000    | 12288  |
| 25       | 2000    | 8192   |



(续)

| 频率实际值/Hz | 十六进制对应值 | 十进制对应值 |
|----------|---------|--------|
| 18.75    | 1500    | 5376   |
| 12.5     | 1000    | 4096   |
| 6.25     | 500     | 1280   |

liquid\_level\_control ▶ PLC\_1 [CPU 314C-2 DP] ▶ 监控与强制表 ▶ 监控表\_1

|   | i | 名称           | 地址     | 显示格式 | 监视值                            | 修改值   |
|---|---|--------------|--------|------|--------------------------------|-------|
| 1 |   | "状态值和实际速度值"  | %MD10  | 十六进制 | 16#FB31_0000                   |       |
| 2 |   | "控制字和设定频率"   | %MD14  | 十六进制 | 16#047E_0000                   |       |
| 3 |   | "START/STOP" | %M20.0 | 布尔型  | <input type="checkbox"/> FALSE | FALSE |

a)

liquid\_level\_control ▶ PLC\_1 [CPU 314C-2 DP] ▶ 监控与强制表 ▶ 监控表\_1

|   | i | 名称           | 地址     | 显示格式 | 监视值                                      | 修改值  |
|---|---|--------------|--------|------|------------------------------------------|------|
| 1 |   | "状态值和实际速度值"  | %MD10  | 十六进制 | 16#FA34_0AD2                             |      |
| 2 |   | "控制字和设定频率"   | %MD14  | 十六进制 | 16#047F_2000                             |      |
| 3 |   | "START/STOP" | %M20.0 | 布尔型  | <input checked="" type="checkbox"/> TRUE | TRUE |

b)

liquid\_level\_control ▶ PLC\_1 [CPU 314C-2 DP] ▶ 监控与强制表 ▶ 监控表\_1

|   | i | 名称           | 地址     | 显示格式 | 监视值                                      | 修改值  |
|---|---|--------------|--------|------|------------------------------------------|------|
| 1 |   | "状态值和实际速度值"  | %MD10  | 十六进制 | 16#FB34_2000                             |      |
| 2 |   | "控制字和设定频率"   | %MD14  | 十六进制 | 16#047F_2000                             |      |
| 3 |   | "START/STOP" | %M20.0 | 布尔型  | <input checked="" type="checkbox"/> TRUE | TRUE |

c)



图 3-48 变频器状态

a) 变频器停止状态 b) 变频器启动过程中 c) 变频器稳定运行中

### 3.6 实训项目 基于 S7-300 PLC 的现场总线系统构建与运行

#### 1. 实训目的

- 1) 了解 PROFIBUS 现场总线控制系统结构。
- 2) 了解 PROFIBUS 技术网络控制方法。
- 3) 学会使用 TIA PORTAL 软件进行系统的硬件组态与通信设置。
- 4) 初步具备 PROFIBUS-DP 现场总线控制系统联机调试的能力。

#### 2. 实训内容

- 1) 控制要求：实现主站与从站之间的通信功能和数据交换功能。
- 2) 使用 TIA PORTAL 软件进行系统的硬件组态和程序设计。
- 3) 联机调试控制系统功能，观察控制系统运行情况。

#### 3. 实训报告要求

- 1) 画出主站与从站之间的数据传送图。



- 2) 写出硬件组态的通信参数设置和实现控制功能的程序。
- 3) 描述并分析项目调试中遇见的问题及解决办法。

### 3.7 思考与练习

1. 阐述 PROFIBUS 现场总线的性能。
2. PROFIBUS 有哪几种传输技术？各有什么特点？
3. PROFIBUS-DP、PROFIBUS-PA 各有什么特性？
4. PROFIBUS 总线存取方式有哪两种？
5. 在 PROFIBUS 网络中，1 类主站起什么作用？哪些设备可以作为 1 类主站？
6. 在 PROFIBUS 网络中，2 类主站有什么作用？列举两种可以作为 2 类主站的设备。
7. PROFIBUS 网络从站设备可以分为几类？列举几种能作为 PROFIBUS 网络从站的设备名称。
8. GSD 文件有什么作用？它包括哪几部分内容？
9. 如何获取和安装 GSD 文件？
10. 硬件组态具有什么特性？
11. 在硬件组态中为什么要保持数据的一致性？
12. DP 主站与智能从站通信的传输区域采用什么区域变量？具有什么特性？
13. MM4 变频器作为 DP 从站时需要配置什么模块？通信变量采用什么区域？
14. 查阅文献，写出在实际生产中 2~3 个应用 PROFIBUS 总线实现控制的系统。