电气信息工程丛书

西门子(中国)有限公司重点推荐图书

SIEMENS

西门子工业通信网络

组态编程与故障诊断

主　编　廖常初

副主编　祖正容

赠送超值DVD光盘：

- 西门子(中国)有限公司授权的通信软件：SIMATIC NET、Drivemonitor、iMap PDM V6.0、S7-PDIAG(不含许可证)
- 100多本中英文用户手册
- 100多个应用实例

机械工业出版社
CHINA MACHINE PRESS

电气信息工程丛书

西门子工业通信网络组态编程与故障诊断

主　编　廖常初
副主编　祖正容

机械工业出版社

本书全面介绍了西门子工业通信网络的结构、通信协议、通信服务和通信的组态编程与故障诊断。重点是应用最广的 PROFIBUS-DP 和工业以太网，对 MPI、AS-i、PROFIBUS-PA、OPC 也作了详细介绍。

本书建立在大量实验的基础上，详细介绍了实现通信最关键的组态和编程的方法，随书光盘有上百个通信例程，绝大多数例程经过硬件实验的验证。读者根据正文介绍的通信系统的组态步骤和方法，参考光盘中的例程作组态和编程练习，可以较快地掌握网络通信的实现方法。

通信的故障诊断是现场维修的难点。本书用约三分之一的篇幅和大量的实例，系统地介绍了网络通信的故障诊断方法、诊断数据的分析方法，和用人机界面、WinCC 显示故障消息的方法，包括一种功能强大、容易实现的故障诊断和显示的方法。

除了例程，“随书光盘还提供了多个西门子大型通信软件和 100 多本中英文用户手册。”本书各章配有适量的练习题，可供工程技术人员和维修人员自学，和作为大专院校、培训班的教材或参考书。

图书在版编目（CIP）数据

西门子工业通信网络组态编程与故障诊断 / 廖常初主编. —北京：机械工业出版社，2009.9

（电气信息工程丛书）

ISBN 978-7-111-28256-3

Ⅰ. 西… Ⅱ. 廖… Ⅲ. 工业—通信网 Ⅳ. TP393.18

中国版本图书馆 CIP 数据核字（2009）第 162962 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

责任编辑：李馨馨

责任印制：洪汉军

三河市国英印务有限公司印刷

2009 年 10 月第 1 版 • 第 1 次印刷

184mm×260mm • 30.75 印张 • 761 千字

0001— 5000 册

标准书号：ISBN 978-7-111-28256-3

ISBN 978-7-89451-204-8（光盘）

定价：69.00 元（含 1DVD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

社服务中心：（010）88361066

销 售 一 部：（010）68326294

销 售 二 部：（010）88379649

读者服务部：（010）68323821

网络服务

门户网：http:///www.cmpbook.com

教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　言

工业控制网络已经成为现代工业控制系统不可缺少的重要组成部分，从计算机、PLC 到现场的 I/O 设备、驱动设备和人机界面，网络通信无处不在。西门子是自动化领域最大的供应商，该公司支持的 PROFIBUS、PROFINET 和 AS-i 已成为 IEC 现场总线国际标准和我国的国家标准。PROFIBUS 已经有两千多万个节点投入运行。

本书对西门子工业通信网络的结构、通信协议、通信服务和通信的组态与编程进行了全面的介绍。对通信中常用的一些基本概念和名词也作了介绍。

本书紧密结合工业通信网络的应用实践，以当前应用最广的 PROFIBUS-DP 和工业以太网为重点。第 2 章介绍了 PROFIBUS 的硬件与通信协议，第 3 章介绍了 DP 主站与 ET 200、智能从站、变频器和直流调速装置等设备之间的主从通信，以及通信处理器在主从通信中的应用。第 4 章介绍了基于 PROFIBUS 的 S7 通信和 FDL 通信，第 5 章介绍了直接数据交换通信和 DP 通信的特殊应用。第 6～8 章介绍了 PROFIBUS 通信的故障诊断与显示的方法。第 9 章介绍了 PROFIBUS-PA，第 10 章介绍了基于工业以太网的 S5 兼容通信和 S7 通信，第 11 章介绍了 PROFINET 通信与工业以太网的故障诊断。第 12 章介绍了 AS-i，第 13 章介绍了 OPC 通信，第 14 章介绍了 MPI 的全局数据通信、S7 基本通信和 S7 通信。第 15 章介绍了点对点通信和 S7 路由，对其他应用较少的通信方式作了简要的介绍。

本书对实现通信最关键的问题——组态与编程作了详细的介绍。全书的内容建立在硬件实验的基础上，随书光盘提供了上百个通信例程，绝大多数例程经过硬件实验的验证，“书中对例程的组态过程、通信程序和验证通信的方法作了详细的说明。”。读者可以一边看书，一边用 STEP 7 打开相应的例程，通过例程了解组态和编程的方法。本书介绍的方法具有很强的可操作性，读者可以根据书中介绍的组态的步骤和方法，同时参考光盘中的例程，做组态和编程的练习，这样可以较快地掌握通信网络的组态和编程方法。有条件的读者可以在看书的同时做一些硬件实验。

现代网络控制系统越来越复杂，网络通信的故障诊断是现场电气维修人员面临的新的巨大的挑战。西门子提供了大量的用于故障诊断和显示的硬件、软件和诊断方法，但是大多数现场维修人员对此知之甚少。本书用了约三分之一的篇幅，通过大量的实例，系统地介绍了网络通信的故障诊断方法，包括用模块上的 LED 和 STEP 7 进行诊断，中断组织块在故障诊断中的应用，用中断组织块的局部变量和通信块的输出参数进行诊断，用通信处理器和专用硬件进行诊断，用诊断程序块进行诊断，诊断数据的分析方法，以及通过全集成自动化（TIA），用人机界面和 WinCC 显示故障消息的方法。另外还介绍了一种功能强大、容易实现的故障诊断和显示的方法——报告系统错误功能。

本书与当前使用的西门子的软件和硬件配套，内容新颖实用。本书的例程基于 STEP 7 V5.4.3.1 中文版和 WinCC flexible 2007 中文版，作者编写的《S7-300/400 PLC 应用技术（第 2 版）》和《西门子人机界面（触摸屏）组态与应用技术（第 2 版）》的随书光盘有这两个软件的演示版。

本书对内容、插图和程序作了优化处理，详细介绍了第一次出现的硬件和网络的组态过

程和通信程序。后面的章节涉及到类似的组态过程和程序时，只作简单的说明。详细的情况可以查看随书光盘的例程中的组态结果和程序代码。这样避免了大量的重复，减少了篇幅，使本书具有很高的性能价格比。建议对硬件组态和网络组态不太熟悉的读者，从第 3 章开始，按书上的顺序阅读组态过程并做组态的练习。

限于篇幅，本书对硬件选型、组网和硬件安装方面的内容介绍得较少。读者可以查阅随书光盘的文件夹“产品样本”中的文档获取有关的信息。

经西门子公司授权，随书光盘有常用的通信软件，以及大量的与通信有关的中英文用户手册。本书的附录有常用缩写词和随书光盘内容简介，各章配有适量的练习题。

本书的编写得到了西门子（中国）有限公司的大力支持，宋柏青先生、元娜、许艳婷女士对本书的编写提供了很大的帮助，在此表示衷心的感谢。

本书由廖常初任主编，祖正容任副主编，陈晓东、陈曾汉、范占华、杨太平、文家学、刘道芳、廖亮、左源洁、万莉、孙明秀、左渊林、王云杰、杨斌、唐永红参加了编写工作。

因作者水平有限，书中难免有错漏之处，恳请读者批评指正。

作者 E-mail：liaosun@cqu.edu.cn。

重庆大学电气工程学院 廖常初

目　录

第1章 概 述

1.1 计算机通信的国际标准

1.1.1 开放系统互连模型

国际标准化组织 ISO 提出了开放系统互连模型 OSI，作为通信网络国际标准化的参考模型，它详细描述了通信功能的 7 个层次（见图 1-1）。

7 层模型分为两类，一类是面向用户的第 5～7 层，另一类是面向网络的第 1～4 层。前者给用户提供适当的方式去访问网络系统，后者描述数据怎样从一个地方传输到另一个地方。

发送方传送给接收方的数据，实际上是经过发送方各层从上到下传递到物理层，通过物理媒体（媒体又称为介质）传输到接收方后，再经过从下到上各层的传递，最后到达接收方的应用程序。发送方的每一层协议都要在数据报文前增加报文头，报文头包含完成数据传输所需的控制信息，只能被接收方的同一层识别和使用。接收方的每一层只阅读本层的报文头的控制信息，并进行相应的协议操作，然后删除本层的报文头，最后得到发送方发送的数据。

1．物理层

物理层的下面是物理媒体，例如双绞线、同轴电缆和光纤等。物理层为用户提供建立、保持和断开物理连接的功能，定义了传输媒体接口的机械、电气、功能和规程的特性。RS-232C、RS-422 和 RS-485 等就是物理层标准的例子。

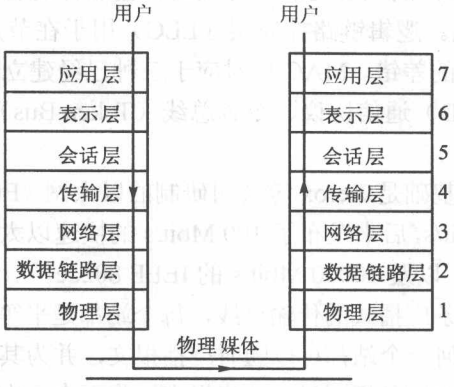

图 1-1 开放系统互连模型

2．数据链路层

数据链路层的数据以帧（Frame）为单位传送，每一帧包含一定数量的数据和必要的控制信息，例如同步信息、地址信息和流量控制信息。通过校验、确认和要求重发等方法实现差错控制。数据链路层负责在两个相邻节点间的链路上，实现差错控制、数据成帧和同步控制等。

3．网络层

网络层的主要功能是报文包的分段、报文包阻塞的处理和通信子网中路径的选择。

4．传输层

传输层的信息传送单位是报文（Message），它的主要功能是流量控制、差错控制、连接支持，传输层向上一层提供一个可靠的端到端（end-to-end）的数据传送服务。

5．会话层

会话层的功能是支持通信管理和实现最终用户应用进程之间的同步，按正确的顺序收发数据，进行各种对话。

6．表示层

表示层用于应用层信息内容的形式变换，例如数据加密/解密、信息压缩/解压和数据兼容，把应用层提供的信息变成能够共同理解的形式。

7．应用层

应用层作为 OSI 的最高层，为用户的应用服务提供信息交换，为应用接口提供操作标准。

不是所有的通信协议都需要 OSI 参考模型中的全部 7 层，例如有的现场总线通信协议只采用了 7 层协议中的第 1、2 和 7 层。

1.1.2 IEEE 802 通信标准

IEEE（国际电工与电子工程师学会）的 802 委员会于 1982 年颁布了一系列计算机局域网分层通信协议标准草案，总称为 IEEE 802 标准。它把 OSI 参考模型的底部两层分解为逻辑链路控制层（LLC）、媒体访问控制层（MAC）和物理传输层。前两层对应于 OSI 参考模型中的数据链路层，数据链路层是一条链路（Link）两端的两台设备进行通信时必须共同遵守的规则和约定。

媒体访问控制层（MAC）的主要功能是控制对传输媒体的访问，实现帧的寻址和识别，并检测传输媒体的异常情况。逻辑链路控制层（LLC）用于在节点间对帧的发送、接收信号进行控制，同时检验传输中的差错。MAC 层对应于三种已经建立的标准，即带冲突检测的载波侦听多路访问（CSMA/CD）通信协议、令牌总线（Token Bus）和令牌环（Token Ring）。

1．CSMA/CD

CSMA/CD 通信协议的基础是 Xerox 等公司研制的以太网（Ethernet），早期的 IEEE 802.3 标准规定的波特率为 10 Mbit/s，后来发布了 100 Mbit/s 的快速以太网 IEEE 802.3u，1000 Mbit/s 的千兆以太网 IEEE 802.3z，以及 10000 Mbit/s 的 IEEE 802ae。

CSMA/CD 各站共享一条广播式的传输总线，每个站都是平等的，采用竞争方式发送信息到传输线上，也就是说，任何一个站都可以随时广播报文，并为其他各站接收。当某个站识别到报文上的接收站名与本站的站名相同时，便将报文接收下来。由于没有专门的控制站，两个或多个站可能因为同时发送信息而发生冲突，造成报文作废，因此必须采取措施来防止冲突。

发送站在发送报文之前，先监听一下总线是否空闲，如果空闲，则发送报文到总线上，称之为“先听后讲”。但是这样做仍然有发生冲突的可能，因为从组织报文到报文在总线上传输需要一段时间，在这段时间内，另一个站通过监听也可能会认为总线空闲，并发送报文到总线上，这样就会因为两个站同时发送而发生冲突。

为了防止冲突，在发送报文开始的一段时间，仍然监听总线，采用边发送边接收的办法，

把接收到的信息和自己发送的信息相比较，若相同则继续发送，称之为“边听边讲”；若不相同则说明发生了冲突，立即停止发送报文，并发送一段简短的冲突标志（阻塞码序列），来通知总线上的其他站点。为了避免产生冲突的站同时重发它们的帧，采用专门的算法来计算重发的延迟时间。通常把这种“先听后讲”和“边听边讲”相结合的方法称为 CSMA/CD（带冲突检测的载波侦听多路访问技术），其控制策略是竞争发送、广播式传送、载体监听、冲突检测、冲突后退和再试发送。

以太网首先在个人计算机网络系统，例如办公自动化系统和管理信息系统（MIS）中得到了极为广泛的应用，以太网的硬件（例如网卡、集线器和交换机）非常便宜。

在以太网发展的初期，通信速率较低。如果网络中的设备较多，信息交换比较频繁，可能会经常出现竞争和冲突，影响信息传输的实时性。随着以太网传输速率的提高（100～1000 Mbit/s）和采用了相应的措施，这一问题已经解决，现在以太网在工业控制中得到了广泛的应用，大型工业控制系统最上层的网络几乎全部采用以太网。使用以太网很容易实现管理网络和控制网络的一体化。

以太网仅仅是一个通信平台，它包括 ISO 开放系统互联模型的 7 层模型中的底部两层，即物理层和数据链路层。即使增加上面两层的 TCP/IP，也不是可以互操作的通信协议。

2．令牌总线

IEEE 802 标准的工厂媒体访问技术是令牌总线，其编号为 802.4。它吸收了通用汽车公司支持的制造自动化协议（Manufacturing Automation Protocol，MAP）的内容。

在令牌总线中，媒体访问控制是通过传递一种称为令牌的控制帧来实现的。按照逻辑顺序，令牌从一个装置传递到另一个装置，传递到最后一个装置后，再传递给第一个装置，如此周而复始，形成一个逻辑环。令牌有“空”和“忙”两个状态，令牌网开始运行时，由指定的站产生一个空令牌沿逻辑环传送。任何一个要发送信息的站都要等到令牌传给自己，判断为空令牌时才能发送信息。发送站首先把令牌置成“忙”，并写入要传送的信息、发送站名和接收站名，然后将载有信息的令牌送入环网传输。令牌沿环网循环一周后返回发送站时，如果信息已被接收站复制，发送站将令牌置为“空”，送上环网继续传送，以供其他站使用。

如果在传送过程中令牌丢失，则由监控站向网内注入一个新的令牌。

令牌传递式总线能在很重的负荷下提供实时同步操作，传输效率高，适于频繁、少量的数据传送，因此它最适合于需要进行实时通信的工业控制网络系统。

3．令牌环

令牌环媒体访问方案是 IBM 公司开发的，它在 IEEE 802 标准中的编号为 802.5，有些类似于令牌总线。在令牌环上，最多只能有一个令牌绕环运动，不允许两个站同时发送数据。令牌环从本质上看是一种集中控制式的环，环上必须有一个中心控制站负责网络的工作状态的检测和管理。

4．主从通信方式

主从通信方式是 PLC 常用的一种通信方式。主从通信网络只有一个主站，其他的站都是从站。在主从通信中，主站是主动的，主站首先向某个从站发送请求帧（轮询报文），该从站接收到后才能向主站返回响应帧。通常主站按事先设置好的轮询表的排列顺序对从站进行周期性的查询，并分配总线的使用权。每个从站在轮询表中至少要出现一次，对实时性要求较高的从站可以在轮询表中出现几次，还可以用中断方式来处理紧急事件。

PROFIBUS-DP 的主站之间的通信为令牌方式，主站与从站之间为主从方式。

1.1.3 现场总线及其国际标准

1. 现场总线的基本概念

IEC（国际电工委员会）对现场总线（Fieldbus）的定义是“安装在制造和过程区域的现场装置与控制室内的自动控制装置之间的数字式、串行、多点通信的数据总线”。它是当前工业自动化的热点之一。现场总线以开放的、独立的、全数字化的双向多变量通信取代 4～20mA 现场模拟量信号。现场总线 I/O 集检测、数据处理、通信为一体，可以代替变送器、调节器、记录仪等模拟仪表，它不需要框架、机柜，可以直接安装在现场导轨槽上。现场总线 I/O 的接线极为简单，只需一根电缆，从主机开始，沿数据链从一个现场总线 I/O 连接到下一个现场总线 I/O。使用现场总线后，可以节约配线、安装、调试和维护等方面的费用，现场总线 I/O 与 PLC 可以组成高性能价格比的 DCS（集散控制系统）。

使用现场总线后，操作员可以在中央控制室实现远程监控，对现场设备进行参数调整，还可以通过现场设备的自诊断功能诊断故障和寻找故障点。

2. IEC 61158

由于历史的原因，现在有多种现场总线标准并存，IEC 的现场总线国际标准（IEC 61158）在 1999 年底获得通过，经过多方的争执和妥协，最后容纳了 8 种互不兼容的协议，这 8 种协议对应于 IEC 61158 中的 8 种现场总线类型：

类型 1：TS 61158，原 IEC 技术报告。

类型 2：ControlNet（美国 Rockwell 公司支持）。

类型 3：PROFIBUS（德国西门子公司支持）。

类型 4：P-Net（丹麦 Process Data 公司支持）。

类型 5：FF 的 HSE（高速以太网，现场总线基金会的 H2，美国 Fisher Rosemount 公司支持）。

类型 6：SwiftNet（美国波音公司支持）。

类型 7：WorldFIP（法国 Alstom 公司支持）。

类型 8：Interbus（德国 Phoenix contact 公司支持）。

2000 年又补充了两种类型：

类型 9：FF H1（美国 Fisher Rosemount 公司支持）；

类型 10：PROFINET（西门子公司支持）。

由于以太网应用非常普及，产品价格低廉，硬件软件资源丰富，传输速率高（工业控制网络已经在使用 1000 Mbit/s 以太网），网络结构灵活，可以用软件和硬件措施来解决响应时间不确定性的问题，各大公司和标准化组织纷纷提出了各种提升工业以太网实时性的解决方案，从而产生了实时以太网（Real Time Ethernet，RTE）。

2007 年 7 月出版的 IEC 61158 第 4 版采纳了经过市场考验的 20 种现场总线（见表 1-1）。其中的类型 1 是原 IEC 61158 第 1 版技术规范的内容，类型 2 通用工业协议（Common Industry Protocol，CIP）包括 DeviceNet、ControlNet 和实时以太网 Ethernet/IP。类型 6 SwiftNet 因为市场应用很不理想，已被撤消。

EPA（Ethernet for Plant Automation，用于工厂自动化的以太网）是我国拥有自主知识产