工业自动化技术与应用丛书

工业控制系统及应用
——SCADA系统篇

王华忠　陈冬青　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

工业自动化技术与应用丛书

工业控制系统及应用
——SCADA 系统篇

王华忠　陈冬青　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书系统地介绍了一类主要的工业控制系统——监督控制与数据采集（SCADA）系统的组成和特点，对 SCADA 系统设计与开发中的关键技术，包括 OPC 规范、I / O 接口与数据采集、IEC 61131-3 编程语言标准、工业控制组态软件、通信与网络技术、控制系统功能安全与信息安全，以及 SCADA 系统集成等做了详实的介绍，并通过对实际应用案例的剖析来加深读者对内容的理解，帮助掌握 SCADA 系统的设计、开发与应用维护技能。此外，对 SCADA 系统开发中的一些典型软、硬件产品及其使用也做了介绍。

本书侧重于 SCADA 系统应用与开发中的关键与主流技术和系统集成及其应用，注重实用性与新颖性。

本书可作为自动化、测控技术及仪器、电气工程及其自动化等相关专业大学本科生、研究生的教材，也可作为工控企业、自动化工程公司相关技术人员的参考书。

图书在版编目（CIP）数据

工业控制系统及应用. SCADA 系统篇 / 王华忠，陈冬青编著. —北京：电子工业出版社，2017.2
（工业自动化技术与应用丛书）

ISBN 978-7-121-30685-3

Ⅰ. ①工… Ⅱ. ①王… ②陈… Ⅲ. ①工业控制计算机 Ⅳ. ①TP273②TP368.4

中国版本图书馆 CIP 数据核字（2016）第 311341 号

策划编辑：陈韦凯
责任编辑：康　霞
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：23.25　字数：595 千字
版　　次：2017 年 2 月第 1 版
印　　次：2017 年 2 月第 1 次印刷
印　　数：3 500 册　　定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254441；bjcwk@163.com。

前　言

典型的工业控制系统包括集散控制系统（DCS）和监控与数据采集系统（SCADA）。SCADA 是英文“Supervisory Control And Data Acquisition”的简称，翻译成中文就是“监督控制与数据采集”，有些文献也称为“监视控制与数据采集”。一般来讲，SCADA 系统特指分布式计算机测控系统，主要用于测控点十分分散、分布范围广泛的生产过程或设备的监控，在通常情况下，测控现场是无人或少人值班，如城市排水泵站远程监控系统、城市煤气管网远程监控、电力行业调度自动化等。SCADA 系统在硬件上不如 DCS 或 FCS 等系统紧凑和专用，但其系统更加开放和多样，组成更加灵活。SCADA 系统在控制层面上至少具有两层结构及连接两个控制层的通信网络，这两层结构是处于测控现场的数据采集与控制终端设备（通常称为下位机——Slaver Computer）和位于中控室的集中监视、管理及远程监控计算机（上位机——Master Computer）。

由于 SCADA 系统的应用领域极其广泛，而不同应用领域的特点和监控要求又导致 SCADA 系统解决方案的多样性和行业应用特征属性，从而导致对 SCADA 系统的认识有所不同。但不论在哪个领域应用，用户对 SCADA 系统的功能要求是一致的。从其名称可以看出，它包含两个层次的基本功能：数据采集和监督控制。因而，SCADA 系统在系统结构、功能、开发工具等方面是有许多共性的，本书正是针对性地介绍 SCADA 系统中的这些共性内容，特别是近些年来控制领域出现的一些新的技术和规范。

《工业控制系统及应用——SCADA 系统篇》共有 9 章，各章主要内容介绍如下。

第 1 章是 SCADA 系统概述，主要介绍什么是 SCADA 系统，系统组成、功能、特点及其应用，对 SCADA 系统与 DCS 和 PLC 也进行了比较，对控制系统功能安全与信息安全做了概述性介绍。

第 2 章是数据通信与网络技术，主要介绍 SCADA 系统中常用的通信手段和技术，由于 SCADA 系统广泛用于测控点较为分散、测控设备分布范围广的领域，因此，实现通信的手段和技术很多，涵盖了目前主流的有线与无线通信。

第 3 章是 I / O 接口与数据采集技术，主要介绍了数据采集中有关输入 / 输出接口知识、SCADA 系统中常用的数据采集方法与编程、基于 Internet 的数据采集等。

第 4 章是工业控制编程语言标准 IEC61131-3 及基于 PC 的控制技术，主要介绍了该标准的产生、特点、基本内容，特别是对公共元素和编程语言做了比较系统的介绍，最后还介绍了几种支持该标准的软件产品。由于基于 PC 的控制技术普通采用 IEC61131-3 标准的编程语言，因此，在本章也对这种控制技术做了介绍。

第 5 章是工业控制组态软件，主要介绍组态软件的产生和发展历史、组态软件的主要功能和组成、主流的组态软件产品及嵌入式组态软件技术，对采用组态软件开发 SCADA 系统人机界面也做了详细介绍。

第 6 章是工业控制数据交换标准——OPC 规范，主要介绍 OPC 规范的产生、特点、主要内容、OPC 的体系结构和 OPC 服务器与客户程序开发及应用，对 OPC UA 规范也做了介

绍，最后给出了 OPC 规范在工控系统模拟仿真中的应用案例。

第 7 章是工业控制系统功能安全与信息安全，除了介绍经典的功能安全特别是安全仪表系统的内容外，还重点介绍了近年来受到极大重视的工控系统信息安全，对其产生的根源、工控系统脆弱性、工控系统安全防护技术等做了详细分析。

第 8 章是 SCADA 系统设计与开发，主要介绍 SCADA 系统开发的原则、步骤、控制策略与 PID 算法、调试与运行、可靠性设计及抗干扰措施等。

第 9 章是 SCADA 系统应用案例分析，介绍了几个富有特色的应用案例。

这 9 章内容中，第 1 章内容是 SCADA 系统概述，第 3、4 章与 SCADA 系统下位机关系比较紧密，而第 5 章与上位机关系紧密，第 2、6 章属于 SCADA 系统中的上、下位机通信内容，第 7 章属于 SCADA 系统安全相关的内容，这些内容都是属于 SCADA 系统开发中的关键技术。第 8 章是关于 SCADA 系统集成技术；而第 9 章是案例分析，综合利用了前 8 章的内容。除了第 9 章外，在第 2 章～第 7 章也都有相应的实例。

本书作者长期从事工业控制系统、工控信息安全相关的教学、科研与工程实践，结合作者在实践中的经验、体会，以及 SCADA 系统相关技术的发展和大量相关的技术文献，编写了本书。

本书由华东理工大学信息学院王华忠和中国信息安全测评中心陈冬青编著。作者感谢两个单位和同事的支持。感谢北京亚控科技、美国 OPTO22、研华科技、上海宝昌自动化等公司提供的技术资料。在编写过程中还参考了许多线上和线下资料，在此也向有关作者表示感谢。

为便于教学，凡采用本书作为教材的，作者免费提供电子教案，可在华信教育资源网（www.hxedu.com.cn）查找本书下载。

由于时间和作者的水平所限，本书疏漏在所难免，恳请读者提出批评建议，以便进一步修订。同时欢迎大家交流讨论，作者的 E-mail 是 hzwang@ecust.edu.cn。

编著者

2016 年 10 月

目　录

第1章 SCADA系统概述

1.1 SCADA系统的概念

SCADA是英文“Supervisory Control And Data Acquisition”的简称，直译成中文就是“监督控制与数据采集”，有些文献也简称为监控系统。国内还有文献翻译成“数据采集与监视控制”。但英文“supervisory”本身不含有“视”的意思，而是监督、管理的含义，因此，把SCADA翻译成“监督控制与数据采集”更加准确。当然，SCADA系统的监控功能是通过人机界面来实现的，即操作人员可以通过人机界面监视被控系统的运行。从SCADA系统名称可以看出，其包含两个层次的基本功能：数据采集和监控。图1.1所示为一个大型油田的SCADA系统，该系统包括位于井口的现场控制层设备（如RTU或PLC）、转接站监控子系统、联合站计算机控制系统（通常采用集散控制系统）和油田中心站监控系统。这种结构在其他类似的各种监控系统中经常可以看到，如城市公用事业（自来水、污水、雨水、燃气）远程监控系统、油气远距离输送控制系统、电力调度自动化系统、交通自动监控系统、通信基站远程监控系统等。

目前对SCADA系统无统一的定义，一般来讲，SCADA系统特指分布式远程计算机测控系统，主要用于测控点十分分散、分布范围广泛的生产过程或设备的监控，通常情况下，测控现场是无人或少人值守。SCADA系统在控制层面上至少具有两层结构以及连接这两层子系统的通信网络，这两层子系统是处于测控现场的数据采集与控制终端设备（通常称为下位机——Slave Computer）和位于中控室的集中监视、管理和远程监控计算机（上位机——Master Computer或Master Terminal Unit）。复杂的SCADA系统可以有多个现场监控中心，每个监控中心与一定数量的现场控制站通信，完成一定范围内设备监控。上一层的调度中心再和现场监控中心通信，对整个现场设备进行远程监控，对整个被控设备、过程进行集中管理。如长距离油气管道远程输送监控系统，就是这样的系统类型。对于重要的远程监控系统，如西气东输SCADA系统这样的关键基础设施工控系统，除了具有常规的现场控制系统，以及多个监控中心外，在通信层还会采取冗余措施以提高系统的可用性，在现场站点还会采用安全仪表系统以降低事故风险从而提高安全性，对于通信系统还进行加密以确保数据的保密性等。

参考国内外的一些文献，这里作者给出一个SCADA系统的定义：SCADA系统是一类功能强大的计算机远程监督控制与数据采集系统，它综合利用了计算机技术、控制技术、通信与网络技术，完成了对测控点分散的各种过程或设备的实时数据采集，本地或远程的自动控制，以及运行过程的全面实时监控、管理、安全控制和故障诊断，并为上级MES系统提供必要的数据接口和支持。

近年来，随着网络技术、通信技术特别是无线通信技术的发展，SCADA系统在结构上

更加分散，通信方式更加多样，系统结构从 C / S（客户机 / 服务器）架构向 B / S（浏览器 / 服务器）与 C / S 混合的方向发展，各种通信技术如数传电台、GPRS、PSTN、VPN、卫星通信等得到更加广泛的应用。

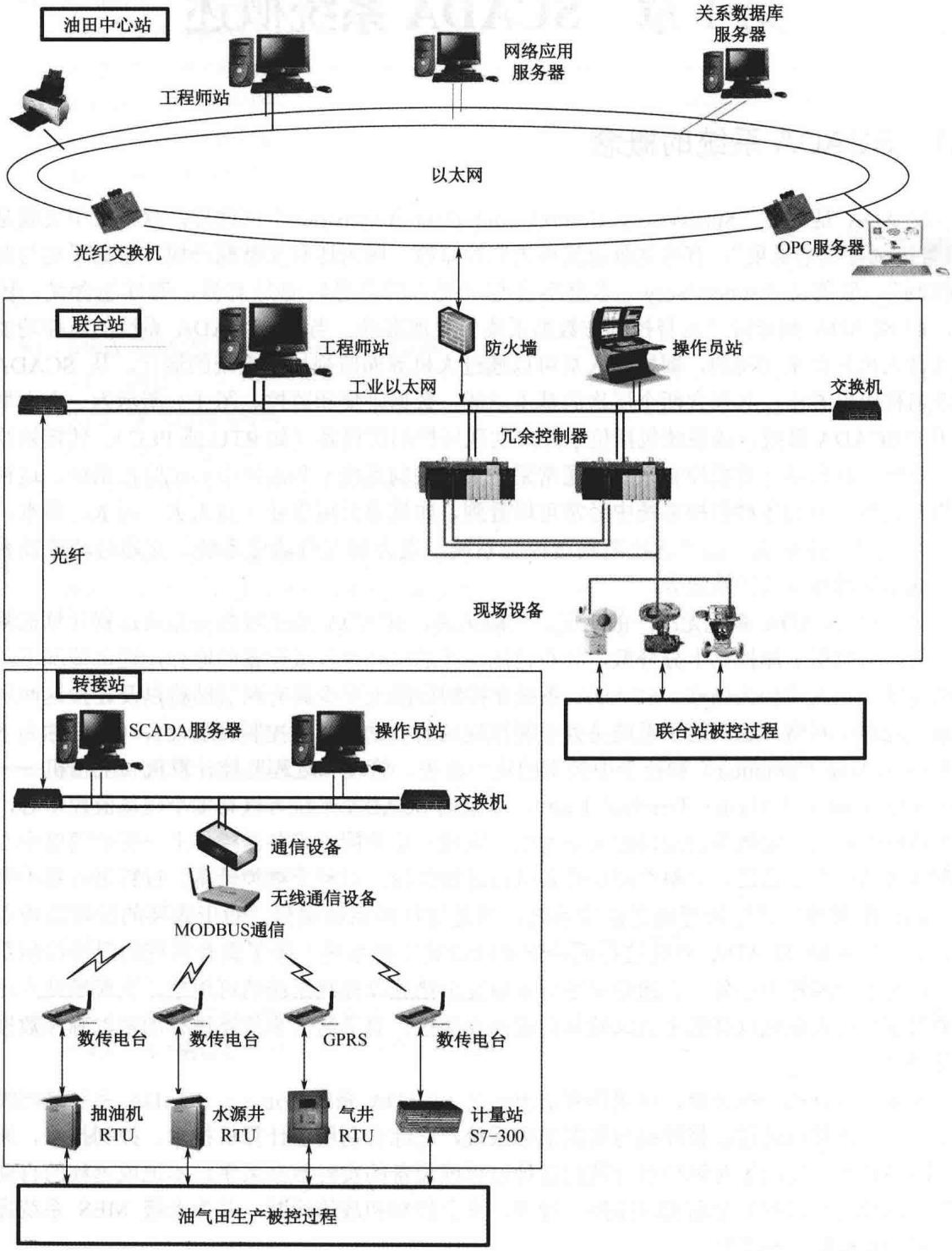

图 1.1　大型油田 SCADA 系统结构示意图

虽然可以采用一台计算机配接各种 I/O 卡件，并且运行自行开发的应用软件也可以实现数据采集与监控，但这类最小规模的系统并不是本书重点要介绍的。当然，本书介绍的内容也同样可以帮助开发这种小型的 SCADA 系统。

1.2 SCADA 系统的组成

SCADA 系统作为生产过程和事务管理自动化最为有效的计算机软硬件系统之一，它包含 3 个部分：第一个是分布式的数据采集系统，也就是通常所说的下位机；第二个是过程监控与管理系统，即上位机；第三个是数据通信网络，包括上位机网络系统、下位机网络，以及将上、下位机系统连接的通信网络。典型的 SCADA 系统的结构如图 1.2 所示。SCADA 系统的这三个组成部分的功能不同，但三者的有效集成则构成了功能强大的 SCADA 系统，完成对整个过程的有效监控。SCADA 系统广泛采用“管理集中、控制分散”的集散控制思想，因此，即使上、下位机通信中断，现场的测控装置仍然能正常工作，确保系统的安全和可靠运行。以下分别对这 3 个部分的组成、功能等作介绍。

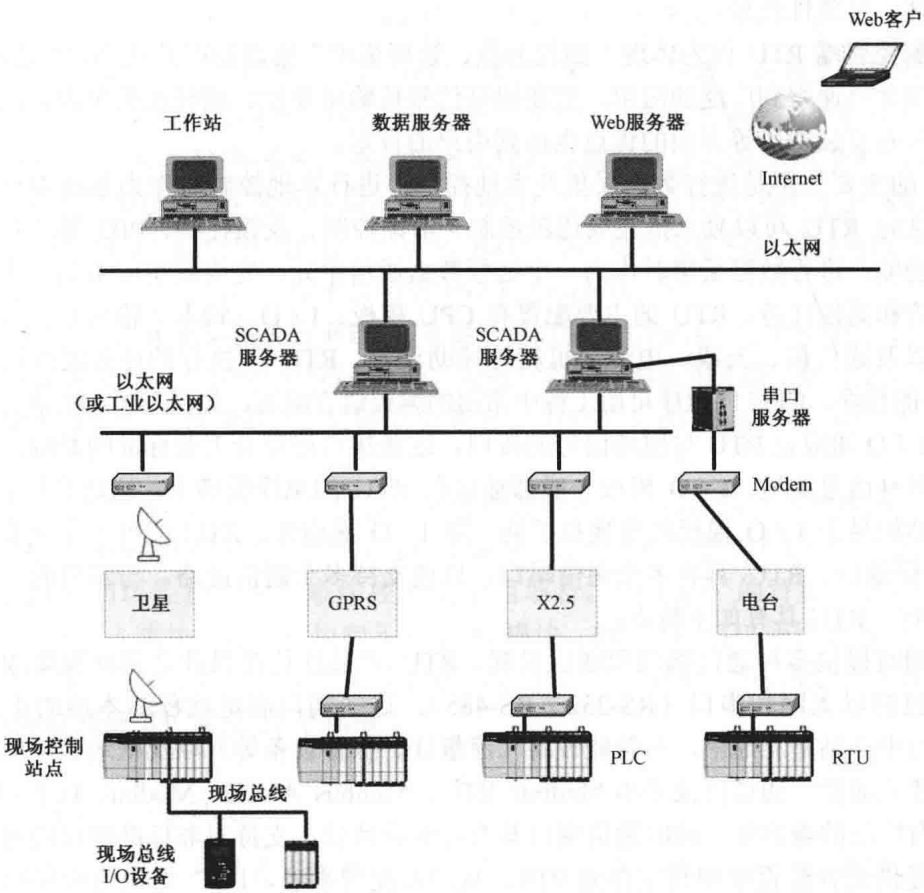

图 1.2 SCADA 系统的结构

1.2.1 下位机系统

下位机一般来讲都是各种智能节点，这些下位机都有自己独立的系统软件和由用户开发的应用软件。该节点不仅完成数据采集功能，而且还能完成设备或过程的直接控制。这些智能采集设备与生产过程各种检测与控制设备结合，实时感知设备各种参数的状态，各种工艺参数值，并将这些状态信号转换成数字信号，并通过各种通信方式将下位机信息传递到上位机系统中，并且接受上位机的监控指令。典型的下位机有远程终端单元 RTU、可编程控制器 PLC、近年才出现的 PAC 和智能仪表等。

1. 远程终端单元 RTU

RTU（Remote Terminal Unit，RTU）是安装在远程现场的电子设备，用来监视和测量安装在远程现场的传感器和设备。RTU 将测得的状态或信号转换成可在通信媒体上发送的数据格式。它还将从中央计算机发送来的数据转换成命令，实现对设备的远程监控。许多工业控制厂家生产各种形式的 RTU，不同厂家的 RTU 通常自成体系，即他们有自己的组网方式和编程软件，开放性较差。

远程测控终端 RTU 作为体现“测控分散、管理集中”思路的产品从 20 世纪 80 年代起介绍到中国并迅速得到广泛的应用。它在提高信号传输可靠性、减轻主机负担、减少信号电缆用量、节省安装费用等方面的优点也得到用户的肯定。

RTU 的主要作用是进行数据采集及本地控制，进行本地控制时作为系统中一个独立的工作站，这时 RTU 可以独立地完成连锁控制、前馈控制、反馈控制、PID 等工业上常用的控制调节功能；进行数据采集时作为一个远程数据通信单元，完成或响应本站与中心站或其他站的通信和遥控任务。RTU 的主要配置有 CPU 模板、I / O（输入 / 输出）模板、通信接口单元，以及通信机、天线、电源、机箱等辅助设备。RTU 能执行的任务流程取决于下载到 CPU 中的程序，CPU 的程序可用工程中常用的编程语言编写，如梯形图、C 语言等。I / O 模板上的 I / O 通道是 RTU 与现场信号的接口，这些接口在符合工业标准的基础上有多种样式，满足多种信号类型。I / O 模板一般都插接在 RTU 的总线板槽上，通过总线与 CPU 相连。这种结构易于 I / O 模板的更换和扩展。除 I / O 通道外，RTU 的另一个重要的接口是 RTU 的通信端口，RTU 具有多个通信端口，以便支持多个通信链路。与常用的工业控制设备 PLC 相比，RTU 具有如下特点：

（1）同时提供多种通信端口和通信机制。RTU 产品往往在设计之初就预集成了多个通信端口，包括以太网和串口（RS-232 / RS-485）。这些端口满足远程和本地的不同通信要求，包括与中心站建立通信，与智能设备（流量计、报警设备等）以及就地显示单元和终端调试设备建立通信。通信协议采用 Modbus RTU、Modbus ASCII、Modbus TCP / IP 等标准协议，具有广泛的兼容性。同时通信端口具有可编程特性，支持对非标准协议的通信定制。

（2）提供大容量程序和数据存储空间。从产品配置来看，PLC 提供的程序和数据存储空间往往只有 6～13KB，而 RTU 可提供 1～32MB 的大容量存储空间。RTU 的一个重要的产品特征是能够在特定的存储空间连续存储 / 记录数据，这些数据可标记时间标签。当通信中断时 RTU 就地记录数据，通信恢复后可补传和恢复数据。

（3）高度集成的、更紧凑的模块化结构设计。紧凑的、小型化的产品设计简化了系统集成工作，适合无人值守站或室外应用的安装。高度集成的电路设计增加了产品的可靠性，同时具有低功耗特性，简化备用供电电路的设计。图 1.3 所示为北京安控科技公司的一体化和模块化 RTU 产品。

（4）更适应恶劣环境应用的品质。PLC 要求环境温度在 0～55℃，安装时不能放在发热量大的元件下面，四周通风散热的空间应足够大。为了保证 PLC 的绝缘性能，空气的相对湿度应小于 85%（无凝露）。否则会导致 PLC 部件的故障率提高，甚至损坏。RTU 产品就是为适应恶劣环境而设计的，通常产品的设计工作环境温度为–40～60℃。某些产品具有 DNV（船级社）等认证，适合船舶、海上平台等潮湿环境应用。

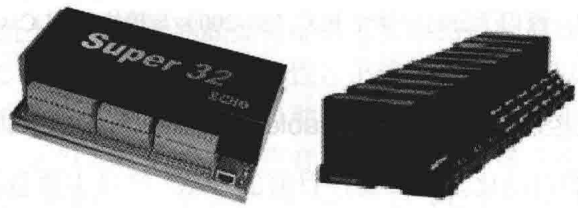

图 1.3　安控科技公司的一体化 RTU 与模块化 RTU

正是由于 RTU 完善的功能，使得 RTU 产品在 SCADA 系统中得到了大量的应用。国内外有许多公司从事相关产品的研发和生产。如美国 SIXNET 公司的VersaTRAK IPm、SiteTRAK RTU、RemoteTRAK RTU等系列产品；美国艾默生过程管理公司的 ROC800、FB107；美国 Motorola 公司的 MOSCAD 远程终端；美国 OPTO 22 公司的 OPTOMUX 及 SNAP；澳大利亚埃波罗（ELPRO）公司的 EP105 一体化 RTU 等；北京安控科技股份有限公司的 Super E40、E50；北京华迅通信电子技术公司的 eNET 无线 RTU 等。

VersaTRAK IPm 是最高级的 RTU 控制器，具有强大的通信功能和编程能力。VersaTRAK IPm 内嵌 Linux 系统，具有源码开放的优点，而控制器的所有应用无需了解 Linux。VersaTRAK IPm 与 SIXNET 的其他 RTU 控制器完全兼容。用户原有的 ISaGRAF 程序无需更改即可应用。

艾默生 ROC800 是基于微处理技术的远程控制器，它可以满足各种现场自动化应用功能。可扩展的 ROC800 可以对站场及远程设备进行远程监视、测量和控制；能够满足需要流量计算、PID 闭环控制和逻辑顺序控制的应用场合。ROC800 的背板支持中央处理单元（CPU）、电源输入模块、通信模块和各种 I / O 模块。ROC800 可以通过最多 4 个 I / O 扩展基架进行扩展。每一个扩展基架带 1 个背板和 6 个 I / O 插槽。当选用了全部 4 个扩展基架时，ROC800 能最多扩展至 27 个插槽。

2. 各种中、小型 PLC

典型的小型 PLC 产品有三菱的 FX_{2N} 系统 PLC、西门子的 S7-200 系统、OMRON 的 CPM1A 等。一些中、大型的 SCADA 系统的下位机会选用中型的 PLC 产品，如三菱的 Q 系列、西门子的 S7-300、A-B 公司的 ControlLogix 和施耐德的 Quantum 系列等。由于这些产品性价比高、可靠性高、编程方便，因此，在各种 SCADA 系统中得到广泛的应用。随着现场总线技术的发展，现场总线在以 PLC 为下位机的系统中应用也不断增长。图 1.4 所示

为西门子公司的 PLC 产品。

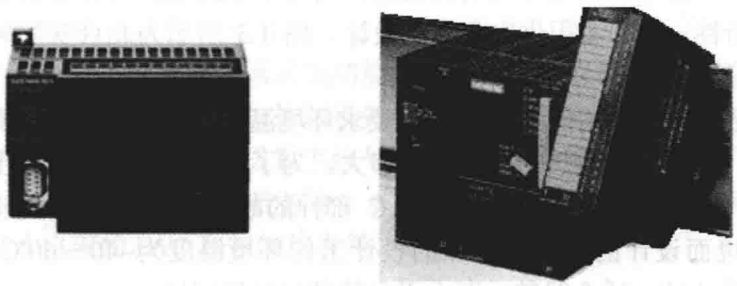

图 1.4　西门子公司一体化 PLC（S7-200）与模块化 PLC（S7-300）

3．可编程自动化控制器（Programmable Automation Controller，PAC）

作为一种开放型的自动化控制设备，目前的 PAC 产品主要包括两类，一类是以研华公司等代表的产品，这些公司进入控制器市场时间不长，没有 PLC 的生产经验，属于控制器市场的后来者。这类公司利用基于 PC 的控制思想和控制系统编程语言标准化的机会，推出了 PAC 产品来抢占控制器市场，典型的产品有研华公司的 ADAM-5510EKW、Beckoff 公司的 CX1000、NI 公司的 Compact FieldPoint、泓格科技的 WinCon / LinCon 系列和μPAC-7186EX 等。另外一类 PAC 厂家是传统的 PLC 制造商，这些公司直接把他们的高端 PLC 就称为 PAC，典型的产品有通用电气公司的 PAC SystemsRX3i / 7i、罗克韦尔公司的 CompactLogix 和 ControlLogix 等。当然，这些厂家也注重这类产品的开放性，如其配套编程软件也能更好地支持 IEC61131-3 编程语言标准。

4．智能仪表

城市公用事业系统如水、电、气的远程监控，热电企业的热网计量与蒸汽计量的远程监控也大量采用 SCADA 系统。与其他一些工业过程的 SCADA 系统相比，它们更加侧重数据采集、信息集中管理与远程监管，而远程控制功能要求较低。在这类 SCADA 系统中，大量使用各种现场仪表做下位机，如智能流量计量表、冷量热量表、智能巡检仪等。还可以采用各种智能控制仪表与传统模拟仪表配套进行计量。采用智能控制仪表后，下位机系统具有更强的控制功能，若不需要控制功能，可以采用具有通信接口的现场仪表直接作为下位机。

不管选用何种形式的下位机，其地位和作用是一样的，它们与生产过程各种检测与控制设备结合，实时感知设备各种参数的状态，各种工艺参数值，并将这些状态信号转换成数字信号，并通过特定数字通信或数字网络传递到上位机系统中；同时，下位机也可根据预先编写的控制程序，完成现场设备的控制。

由于 SCADA 系统中上、下位机的通信可能中断，因此要求下位机系统具有自主控制能力。此外，对于 I / O 模块，也要求具有安全值设置等功能。如 PLC 和一些 RTU 的 I / O 模块可以设置初始状态，或程序停止运行时的输出状态。这些功能在目前许多总线式 I / O 模块中也得到了体现，如泓格 7000 系列部分 I / O 模块，除了可以设置 RS-485 通信中断时的