SIEMENS

西门子工业自动化系列教材

西门子S7-300/400 PLC 编程与应用

刘华波　何文雪　王　雪　编著

第2版

附赠电子教案

http://www.cmpedu.com

附光盘

附软件：

STEP7 V5.5+S7-PLCSIM V5.4+应用文档

机械工业出版社
CHINA MACHINE PRESS

西门子工业自动化系列教材

西门子 S7-300/400 PLC 编程及应用

第 2 版

刘华波　何文雪　王　雪　编著

机 械 工 业 出 版 社

本书由浅入深地全面介绍了西门子公司广泛应用的大中型 PLC——S7-300/400 的编程与应用，注重示例，强调应用。全书共 14 章，分别介绍了 S7 系统概述、硬件安装与维护、编程基础、基本指令、符号功能、测试功能、数据块、结构化编程、模拟量处理及闭环控制、组织块、故障诊断、文档处理和通信网络等。

本书可作为高等院校自动化、电气控制、计算机控制及相关专业的教材，也适合职业学校学生及工程技术人员培训及自学使用，对西门子自动化系统的用户也有一定的参考价值。

本书配有电子课件，需要的教师可登录 www.cmpedu.com 免费注册、审核通过后下载或联系编辑索取（QQ：308596956，电话：010-88379753）。

图书在版编目（CIP）数据

西门子 S7-300/400 PLC 编程与应用 / 刘华波，何文雪，王雪编著．—2 版．—北京：机械工业出版社，2015.4
西门子工业自动化系列教材
ISBN 978-7-111-50141-1

Ⅰ．①西…　Ⅱ．①刘…　②何…　③王…　Ⅲ．①plc 技术－教材
Ⅳ．①TM571.6

中国版本图书馆 CIP 数据核字（2015）第 091982 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：时　静
责任编辑：时　静　刘　悦　　责任校对：张艳霞
责任印制：李　洋

涿州市京南印刷厂印刷

2017 年 1 月第 2 版 • 第 2 次印刷

184mm×260mm • 21.5 印张 • 529 千字

3501－6000 册

标准书号：ISBN 978-7-111-50141-1
　　ISBN 978-7-89405-829-4（光盘）

定价：49.80 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	网络服务
服务咨询热线：010-88379833	机 工 官 网：www.cmpbook.com
读者购书热线：010-88379649	机 工 官 博：weibo.com/cmp1952
	教育服务网：www.cmpedu.com
封面无防伪标均为盗版	金　书　网：www.golden-book.com

前　言

西门子 S7 系列 PLC 广泛应用于工业生产。S7-300/400 系列大中型 PLC 作为其典型代表深受广大用户欢迎。本书第 1 版已问世五年多，在此期间，西门子公司又针对市场需求开发了部分新产品，编程软件版本也有了升级改进，故对此书进行修订是很有必要的。

本书仍由 14 章组成，全面介绍了 S7-300/400 PLC 的硬件、编程和维护及应用等。第 1 章介绍了全集成自动化和 S7 家族产品以及编程软件和授权的安装与设置等，增加了新产品 S7-200 SMART、S7-1200 和 S7-1500 的介绍；第 2 章介绍了 S7-300/400 PLC 的硬件组成、安装维护步骤等；第 3 章介绍了 S7-300/400 PLC 编程的基础知识，包括 PLC 的工作原理、存储区寻址、数据类型、编程方法、编程原则等；第 4 章通过一个简单的实例介绍了 SIMATAIC 管理器的使用、硬件组态的步骤及仿真软件的使用等；第 5 章介绍了 S7-300/400 PLC 的指令系统；第 6 章和第 7 章分别介绍了符号功能和测试功能；第 8 章介绍了数据块的使用；第 9 章介绍了编程方法，重点是模块化编程和结构化编程，增加了部分实例；第 10 章介绍了模拟量的处理及闭环控制；第 11 章介绍了组织块的使用；第 12 章介绍了故障诊断的各种工具及方法；第 13 章简要介绍了文档处理和项目管理的内容；第 14 章介绍了 S7-300/400 PLC 的通信网络及组态步骤。

第 2 版仍由刘华波、何文雪和王雪编写。刘华波进行了第 1、3、4、8、9、12、14 章的修订工作，何文雪进行了第 2、5、6、7 章的修订工作，王雪进行了第 10、11、13 章的修订工作，全书由刘华波统稿。

自本书第 1 版以来，西门子（中国）有限公司的各位同仁皆给予了大力支持，提供了大量资料，提出了宝贵建议。此外，机械工业出版社编辑也提出了很多有价值的建议，在此一并表示衷心的感谢。

本书的编写注重理论和实践相结合，强调基本知识与操作技能相结合。书中提供了大量的实例，读者在阅读过程中应结合实践加强练习，举一反三，系统掌握。

因作者水平有限，书中难免有错漏及疏忽之处，恳请读者批评指正。

作者 E-mail：liuhuabo1979@qdu.edu.cn。

编者

目　录

第 1 章　S7 系统概述

1.1　全集成自动化（TIA）

西门子公司作为全球领先的自动化系统集成商，一直以其先进的自动化技术与产品向用户提供可靠的自动化解决方案。全集成自动化技术（Totally Integrated Automation，TIA）是西门子公司自动化系统技术与产品的核心思想和主导理念。

已有的自动控制解决方案混合了许多不同的技术和厂商，系统使用完全不同形式的软件和用户界面，时常会导致通信问题的发生，而且数据需要多次进行读写，这就迫切需要一种相容的技术来解决这些问题。全集成自动化立足于一种新的概念以实现工业自动控制任务，解决现有的系统瓶颈。

TIA 是西门子公司于 1997 年提出的崭新的革命性的概念，将所有的设备和系统都完整地嵌入到一个彻底的自动控制解决方案中，采用共同的组态和编程、共同的数据管理和共同的通信。图 1-1 所示为全集成自动化示意图。

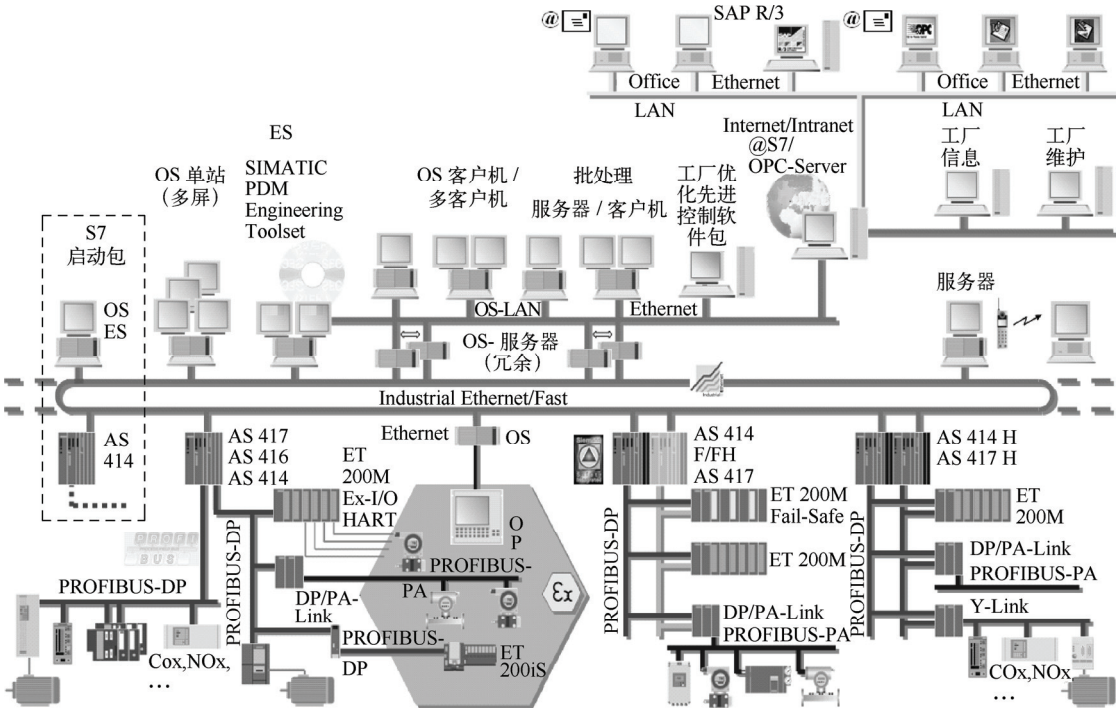

图 1-1　全集成自动化示意图

TIA 集高度的统一性和充分的开放性于一身，标准化的网络体系结构、统一的编程组态环境和高度一致的数据集成，使 TIA 为企业实现了横向和纵向的信息集成；领先的通信标准、基于组件的自动化技术（CBA）与 IT 集成，使 TIA 对全球自动化市场的产品和服务范围真正开放。

1.1.1 TIA 的统一性

通过全集成自动化，可以实现从自动化系统及驱动技术到现场设备整个产品范围的高度集成，其高度集成的统一性主要体现在以下三个方面。

1．统一的数据管理

TIA 采用全局统一的数据库，数据只被写入一次，然后由系统为用户管理，SIMATIC 工业软件家族都从一个全局共享的统一的数据库中获取数据。这种统一的数据管理机制，不仅可以减少输入阶段的费用，还可以降低出错率，提高系统诊断效率，从而对工厂的平稳运行产生积极作用，节省了用于数据格式一致性检查的费用。

TIA 统一的数据管理功能具体体现在以下几个方面。

（1）TIA 统一的符号表

无论使用 SIMATIC 家族中的哪个组态软件，都可以通过全局数据库共享一个统一的符号表。

（2）变量名自动映射

SIMATIC HMI 工具可以自动识别和使用 STEP 7 中定义的变量，并可以与 STEP 7 中变量的改变自动同步。

（3）多用户功能

随着项目规模的增大，多用户功能是必不可少的。TIA 可以方便地实现多用户在同一个项目下工作，同时还可以保证项目的一致性。另外，TIA 还提供了多项目（Multi Project）的管理，使不同团队的分工协作更加方便。

2．统一的编程和组态

在 TIA 中，所有的 SIMATIC 工业软件都可以互相配合，实现了高度集成。组态和编程工具也出自同一模式，只需从全部列表中选择相应的项，即对控制器进行编程、组态 HMI、定义通信连接或实现动作控制等操作。

TIA 统一的编程和组态具体体现在以下几个方面。

（1）统一的界面

SIMATIC 工业软件家族具有统一友好的界面。通过集成安装，可以在 SIMATIC 管理器的统一界面下工作，在 STEP 7 中直接调用其他软件。这种界面的一致性和集成性大大方便了对整个 TIA 系统的编程和组态。

（2）面向对象的“块”概念

SIMATIC 软件中基于面向对象思想的“块”的概念，实现了统一的项目结构，使用户程序的可重用性大大提高，从而避免了大量重复的劳动。

（3）平台无关的编程

统一的编程还实现了平台的无关性，用户程序在基于 PLC 的控制系统和基于 PC 的控制系统中都能运行。这给程序的移植带来了很大的方便，也使得用户在选择解决方案时可以更加灵活。

3．统一的通信网络

TIA 实现了从控制级到现场级协调一致的通信，采用不同功能的总线涵盖了几乎所有的应用：工业以太网和 PROFIBUS 网络是安装技术集成的重要扩展，而 EIB 用于楼宇控制系统的集成。

TIA 统一的通信具有以下特点。

（1）工业以太网和 PROFIBUS 统一的网络组态

在 SIMATIC 中，工业以太网和 PROFIBUS 采用统一的组态，当网络连接发生改变时，可以方便地进行修改。

（2）基于 PROFIBUS 的分布式 I/O

基于 PROFIBUS 的分布式 I/O 与本地 I/O 的组态采用了统一的方式，因此在编程时无需分辨 I/O 类型，而是可以像使用本地 I/O 一样方便地使用分布式 I/O。

（3）系统中集成的路由功能

TIA 中的各种网络可以进行互联。TIA 中集成的路由功能可以方便地实现跨网络的下载、诊断等，使整个系统的安装调试更加容易。

（4）集成的系统诊断和报告功能

TIA 系统集成了自动诊断和错误报告功能，诊断和故障信息可以通过网络自动发送到相关设备而无需编程。

1.1.2 TIA 的开放性

TIA 是一个高度集成和统一的系统，同时也是一个高度开放的系统。TIA 的开放性体现在以下几个方面。

1．对所有类型的现场设备开放

通过 PROFIBUS，TIA 对范围极广的现场设备开放。目前，该总线已经实现了在防爆环境的应用和与驱动设备同步。开关类产品和安装设备还可以通过 AS-I 总线接入自动化系统作为 PROFIBUS 总线的扩展。楼宇自动化与生产自动化的连接则可以通过 EIB 实现。

2．对办公系统开放并支持 Internet

以太网通过 TCP/IP 将 TIA 与办公自动化应用及 Internet/Intranet 相连接。TIA 采用 OPC 作为访问过程数据的标准接口，通过该接口，可以很容易地建立所有基于 PC 的自动化系统与办公应用之间的连接，而不论它们所处的物理位置如何。Internet 技术使在任意位置对工厂进行远程操作和监视成为可能。

3．对新型自动化结构开放

自动化领域中的一个明显的技术趋势就是系统的模块化程度大大提高，即由带有智能功能的技术模块组成的自动化结构。这些模块可以预先进行组态、启动和测试。这样，实现整个工厂的投运要快得多，更改系统也不会影响到生产运行。通过 PROFINET，TIA 使用与厂商无关的通信、自动化和工程标准，系统使用智能仪表非常容易，不必关心它们是否与 PROFIBUS 或者以太网相连接。通过新的工程工具，TIA 实现了对这种结构简单而集成化的组态。

1.2 SIMATIC S7 系列概述

SIMATIC 是西门子自动化系统的缩写，为西门子公司的注册商标。SIMATIC 包括 SIMATIC 控制器、SIMATIC PG 和 PC 等编程设备、SIMATIC HMI 人机界面、SIMATIC DP 以及 SIMATIC NET 等，如图 1-2 所示。

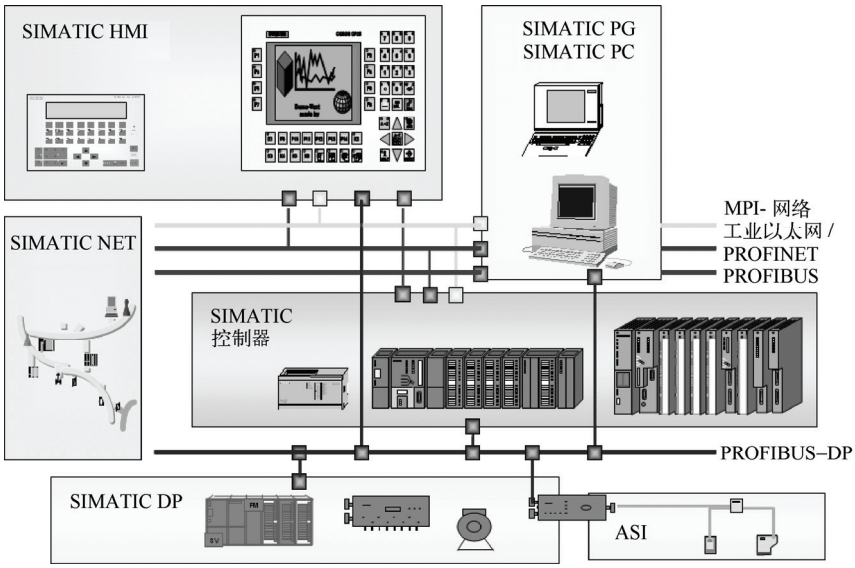

图 1-2 SIMATIC 家族示意图

SIMATIC 控制器包括 SIMATIC S7/C7/M7 及 WinAC 等控制器。SIMATIC S7 PLC 是在 S5 系列 PLC 基础上于 1995 年陆续推出的，后面将详细介绍。

SIMATIC M7 PLC 系统将 AT 兼容机的性能引入 PLC 或将 PLC 的功能加入计算机中并保持熟悉的编程环境。M7-300 和 M7-400 自动化计算机通过开放硬件和软件平台的方法扩展了 PLC 的功能，它们包括一个 AT 兼容机，并在实时多任务操作系统 RMOS 支持下工作。M7 总是用于需要高的计算性能、数据管理和显示的场合。目前，西门子公司已经不再推广该产品。

SIMATIC C7 系列的完整系统是由一个 PLC（S7-300）、一个 HMI 操作面板和过程监视系统组成，它将 PLC 与操作面板集成在一起，可使整个控制设备体积更小、价格更优。

WinAC 是一个基于计算机的解决方案，用于各种控制任务（控制、显示、数据处理）都由计算机完成的场合，主要包括 3 种产品：WinAC Basic 是纯软件的解决方案（PLC 作为 Windows 的任务）；WinAC Pro 是硬件解决方案（PLC 作为 PC 卡）；WinAC FI Station Pro 是完全解决方案（SIMATIC PC FI25）。

SIMATIC S7 PLC 主要包括 S7-200 微型 PLC、S7-300 较低性能 PLC 和 S7-400 中高性能 PLC。S7 系列 PLC 具有模块化、无风扇的结构，使之成为各种由小规模到大规模应用的首选产品，提供了完成控制任务既方便又经济的解决方案。