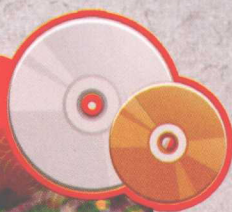


附光盘



可编程序控制器 与工业现场总线

陈忠华○编著



 机械工业出版社
CHINA MACHINE PRESS



可编程序控制器与 工业现场总线

陈忠华 编著



机械工业出版社

本书对 PLC 的硬件体系、工作原理、组态方法、编程语言、模块化结构编程、梯形图指令系统、调试手段和故障诊断,作了全面详细的介绍。对 20 世纪 80 年代产生并迅速发展的工业现场总线,以 IEC 61158 标准中应用广泛的 PROFIBUS_DP 和 PROFINET 两个类型为代表,进行了深入的介绍,说明了 DP_V0、DP_V1 和 DP_V2 3 个标准版本、PROFINET 的基本概念,特别提供了应用现场总线实现 PLC 和伺服驱动装置之间的通信实例,并对该实例进行了详细分析和解读。

本书适合作为高等院校自动化相关专业的教材或教学参考书,对从事自动化领域的工程技术人员、设计人员和设备维修人员也有很高的参考价值。

图书在版编目 (CIP) 数据

可程序控制器与工业现场总线/陈忠华编著. —北京:机械工业出版社, 2010. 4

ISBN 978-7-111-29884-7

I. ①可… II. ①陈… III. ①可程序控制器②总线—技术
IV. ①TM571.6②TP336

中国版本图书馆 CIP 数据核字 (2010) 第 032152 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: 朱 林 责任编辑: 朱 林

版式设计: 霍永明 责任校对: 陈立辉

封面设计: 陈 沛 责任印制: 乔 宇

北京瑞德印刷有限公司印刷 (三河市胜利装订厂装订)

2010 年 5 月第 1 版第 1 次印刷

184mm×260mm·19.75 印张·487 千字

0001-3000 册

标准书号: ISBN 978-7-111-29884-7

ISBN 978-7-89451-440-0 (光盘)

· 定价: 49.00 元 (含 1CD)

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

社服务中心: (010)88361066

门户网: <http://www.cmpbook.com>

销售一部: (010)68326294

教材网: <http://www.cmpedu.com>

销售二部: (010)88379649

读者服务部: (010)68993821

封面无防伪标均为盗版

序 言 1

2009 年底, 陈忠华教授邀请我为他的新书《可编程序控制器与工业现场总线》作序, 不胜荣幸。此书姐妹篇《可编程序控制器与工业自动化系统》自 2006 年出版后受到工业自动化行业读者普遍好评。此次新书, 是经过陈教授精心修订、补充, 特别是根据自动化工程师的实际需要, 增添了近年来兴起的工业现场总线技术内容。本书特点是将可编程序控制器 (PLC) 应用技术与工业现场总线技术相结合, 论述详尽, 内容上融会贯通, 符合当前自动化技术应用现状, 是自动化工程师难得的技术参考及工具书。

现场总线技术概念产生于 20 年前, 在国内有近十几年快速发展历史。现场总线技术迎合了近年来制造业信息化、工厂数字化的技术需求, 为工厂自动化底层现场设备联网、实现底层生产设备信息集成提供了技术平台。现代工厂自动化技术不单纯追求提高单机设备自动化水平, 而是注重整个工厂自动化系统的效率和企业市场竞争提供的支持。现场总线技术的应用为整个工厂实现数据纵向透明传输, 为 MES (Manufacturing Execution System, 制造执行系统)、ERP (Enterprise Resource Planning, 企业资源计划) 提供技术平台。因此, 现场总线技术不是单纯用来提高单机生产设备的自动化水平, 而是为整个工厂数字化、信息化建设提供技术基础, 进而为企业提高经济效益和市场竞争力做出贡献, 这便是近年来现场总线技术应用飞速发展的根本原因。

现场总线技术, 简而言之, 就是控制器 (如 PLC) 与工业现场设备 (如传感器、执行器、驱动装置、专用控制器、人机界面等) 之间的连接不采用一对一的 I/O 连线, 而是通过工业数字通信网络——现场总线, 将所有现场设备与控制器连接, 采用数字通信方式 (而不是 4~20mA 或开关量信号) 实现控制器对现场设备的数据采集和控制。

现场总线技术的产生使整个自动化系统发生结构性变革。比如 PLC 技术与现场总线技术的结合使 PLC 的功能定位发生了很大变化。由于 PLC 可采用现场总线连接现场设备 (如变频器、传感器、控制面板等) 并通过远程 I/O 来替代本地机架 I/O 扩展, 因此, I/O 规模不再是 PLC 的关键指标。通信能力、指令执行速度、功能可扩展性、安全性、信息处理能力等成为 PLC 的关键技术性能。在基于现场总线的控制系统中, 系统主 PLC 更多地被称为控制器; 而具备现场总线通信接口的小型 PLC 可能会向专用控制器方向发展。

实现现场总线技术的前提不仅要求现场设备必须智能化, 而且要求通信接口必须遵守统一的通信协议标准。所以, 在现场总线技术的发展过程中, 现场总线通信协议标准就成为此项技术的关键所在, 也是不同企业技术联盟激烈竞争的制高点。

据统计, 现场总线技术兴起初期, 国际上存在近百种现场总线技术标准。这种局面使最终用户和产品开发制造企业都面临巨大的技术风险。因此, 当时自动化行业迫切希望国际标准化组织能够提出一种适用于自动化行业技术特点、国际上统一的现场总线技术标准。1985

年,国际电工委员会(IEC)成立工业控制网络通信协议标准化工作组着手 IEC61158 标准的制订。工作组目标旨在提出一种能适用于工业自动化领域的、统一的工业控制网络通信协议标准,此后十多年过去了,并没有达到预计的目标。2000 年,工作组选择了当时技术和市场上均比较成熟的几种现场总线技术标准进行整合,提出了一个包括 8 种现场总线技术的 IEC61158 标准(后发展为 10 种)作为国际 IEC 现场总线技术标准。对此陈教授在本书中有详细描述。造成这种局面的原因不单纯是由于不同国际企业技术联盟的商业利益,主要是还由于当时 IEC 工作组没有充分估计到不同行业自动化对现场总线技术要求的不同。从这里我们得到启示是:自动化行业与 IT 行业不同,不可能用一种现场总线技术标准覆盖所有自动化行业的应用需求。各种现场总线技术标准各有技术特点,自有它在各自领域的存在价值。后来兴起的工业以太网技术,其技术标准的发展也同样沿袭了当年现场总线技术标准的老路。目前在 IEC61158 注册的工业以太网标准就有近 5 种。因此,多种技术标准并存,市场竞争与用户选择是我们将长期面对的现状。多年以来在我国,各种现场总线及工业以太网技术经过市场竞争与用户筛选,时至今日,主要流行的工业控制网络技术有:应用在离散制造工业、混合制造工业、轨道交通、基础设施建设等行业的现场总线技术是 PROFIBUS-DP、DeviceNet,工业以太网有 MODBUS/TCP、PROFINET、Ethernet/IP;主要应用在连续制造工业、混合制造工业的现场总线有 FF 和 PROFIBUS-PA。这些技术标准背后有强大的企业技术组织的支持与维护,产品品种、生产厂商、研发机构众多;经过多年的市场竞争与用户筛选,在我国自动化市场上占有明显优势。

本书涉及的现场总线 PROFIBUS 技术始于 1984 年的欧洲,先后成为德国工业标准、欧洲标准,2000 年成为国际 IEC61158 现场总线标准的 Type 3 部分。PROFIBUS 技术是国际上发展和推广非常成功的主流现场总线技术。究其原因,除协议标准及产品的技术因素之外,主要还是依靠了 PROFIBUS 国际组织(PI)的作用。根据最新资料表明,PROFIBUS 国际组织(PI)有 1200 多个企业会员。PI 在国际上设立 4 条主线来完成技术、市场、培训的推广工作。一是地区性组织:PI 在全球与 26 个技术组织建立合作关系成为地区性 PI 组织(Regional PI Associations, RPA),RPA 负责本地区的 PROFIBUS 市场工作。二是资格中心:PI 在全球对 40 个企事业单位、研究机构、学校进行资格认定,成为 PROFIBUS 国际组织资格中心(PI Competence Centers, PICC),PICC 负责地区的技术推广并作为 RPA 的技术支持。三是产品测试实验室:PI 全球设有 10 个 PROFIBUS 国际组织产品测试实验室(PI Test Laboratories for Certification Tests, PITL),这些实验室各有不同的测试业务,主要任务是负责为所在地区企业自主开发 PROFIBUS 产品提供技术支持和产品测试与认证服务。四是 PROFIBUS 培训中心:目前全球有 18 个 PROFIBUS 国际组织培训中心(PI Training Centers, PITC),PITC 负责所在地区 PROFIBUS 工程师培训与认证工作。PI 依靠这 4 条主线,成功地将 PROFIBUS 技术应用推广到世界各地。据统计,截止到 2008 年全球 PROFIBUS 安装站点超过 2300 万个,成为国际市场上应用最广泛的现场总线技术。

PROFIBUS 是引入我国较早,也是目前应用最广、市场占有率最高的现场总线技术。中国机电一体化技术应用协会现场总线专业委员会,又名“中国 PROFIBUS 用户组织”(China PROFIBUS User Organization, CPO)是 PI 在我国的地方性组织。CPO 于 1997 年成立,十多年来,为 PROFIBUS 技术在我国推广做了卓有成效的工作。目前,在我国设有 2 个资格中心(北京鼎实创新科技有限公司、机械工业仪器仪表综合技术经济研究所)、2 个

产品测试实验室（中国机电一体化技术应用协会、机械工业仪器仪表综合技术经济研究所）和一个培训中心（郑州轻工业学院）。这些资格中心、产品测试实验室和培训中心在 CPO 领导下，为我国 PROFIBUS 技术人才的培养，为推动我国企业自主开发 PROFIBUS 技术产品做出了很大贡献。

陈忠华教授在自动化领域享有盛名，他知识渊博，实际经验丰富。本人与陈教授交往近 20 年，在技术上经常受到陈教授指点。无论多复杂的难题，在陈教授那里总是可以得到完整的答案。如今陈教授已退休，我也早已步入中年，但每当回忆起陈教授给予的帮助，心里都充满感激之情。借此机会衷心祝愿陈教授生活幸福，健康长寿！

中国 PROFIBUS 用户组织（CPO）

主席：唐济扬

2010 年 4 月

序 言 2

众所周知,可编程序控制器(PLC)的应用是自动化控制领域的核心技术之一,自产生以来,经过40多年的不断发展,特别是随着半导体芯片技术、计算机技术和数字化控制理论的发展,PLC技术日臻成熟,功能日臻强大,可靠性不断提高,已越来越受到人们的重视。由于PLC系统构成简单、配置灵活、编程方便、可靠性高,能适用于不同类型的控制对象和各种复杂环境,已经在自动化控制领域获得了非常广泛的应用。

在国际上,PLC国际标准IEC 61131的形成和不断修订更新,表明PLC技术的标准化和技术发展的重要性已成为各工业化国家的共识。我国也有着相应的国家标准。此外,今后我国的有关部门将逐步在工业自动化产品领域推行强制安全标准,PLC也将被纳入其中,届时我国的PLC产品和技术的应用也将进入一个新的阶段。

与此同时,自20世纪80年代以来,随着自动化技术的进步和自动化程度的不断提高,自动化系统和设备之间的通信需求也在不断增长,特别是随着计算机网络技术的迅速发展和生产信息化程度的提高,现场总线技术在自动化控制领域中的应用应运而生。

现场总线是一种串行、多点的数字通信技术,它可在自动化控制设备间建立实时的、工业级的互连网络,形成了一种全分布、全数字、全开放的新型控制系统。现场总线技术的先进性、开放性、通用性,使它自产生的那一天开始,就引起了自动化控制工程领域的技术人员和广大用户的高度关注,它的开放性和标准化使不同厂商生产的设备可以方便地实现互连、互换、互操作,给生产商、系统集成商、用户都带来了极大的方便。现场总线技术是自动化控制领域的一项重要创新,它代表了工业自动化网络技术的发展方向,PROFIBUS和PROFINET就是其中的两种。

值得一提的是,我国在2001年就开始筹建国内第一个PROFIBUS产品测试实验室,当年通过了PROFIBUS国际组织专家的验收,成为除欧美外最早开展测试业务的国际性PROFIBUS产品测试实验室。几年来,实验室承接了境内、外许多客户,包括一些国际知名厂商的产品测试业务,并定期参加相关国际会议和各种技术交流,与国内外同行保持着密切的交往和联系,为PROFIBUS技术标准在我国的推广应用提供了可靠的保障。

陈忠华教授早年毕业于上海交通大学电机工程系,在自动化控制工程领域工作近50年,在PLC控制技术、电气传动技术、现场总线技术等方面均有深厚的造诣和丰富的实际经验。是国内工业自动化行业内的资深专家。现虽已年逾七旬,但仍以敏锐的目光和执着的精神,研究、追踪着国际上自动化领域的发展方向和最新的主流技术,并结合国内实际需要,不断地将新的技术应用于实际的工程项目中。此外,陈教授除了经常出现

在控制工程的现场和第一线，对年轻的工程师们进行指导和帮助外，还经常结合实例，在各种培训讲座和学习班上为客户和其他学员讲课，传授他多年的积累和宝贵的经验，为他所热爱的自动化事业继续发挥着光和热。

本书中陈忠华教授介绍了可编程序控制器（PLC）系统和现场总线技术的发展过程、基本概念、工作原理和软硬件的基本构成。并以 SIEMENS 公司 PLC 系统为样本，详细介绍了 STEP7 编程语言的指令系统和编程方法。书中还结合现场总线技术，举例说明了 PLC 控制系统的配置和通信编程方法，并用大量的图片和文字对实例进行了非常详尽和具体的描述。陈忠华教授在编写和调试编程实例时对细节部分的查证和孜孜以求的精神，令人十分感动。书中的许多实例和问题源自陈忠华教授以往的工程实践，或授课学员，因此具有很强的实用性，书中的分析和解读深入浅出，使本书既适合初学者，对希望更深层次地了解 PLC 和工业现场总线技术的工程人员来说，也是极有价值的一本参考书。

中国 PROFIBUS 技术资格中心主任

孙慧民

2010 年 4 月

前 言

本书是作者所著《可编程序控制器与工业自动化系统》一书的姐妹篇，《可编程序控制器与工业自动化系统》自出版以来，深受广大读者的欢迎。本书是为满足读者们的要求，对原书做了若干重大修改和补充。又为了避免改版后的篇幅过于冗长，新书只保留了原书的第1和第2章，另外专门增加1章，对原书第3和第5章也都作了修改并补充了很多新内容，新书特别突出了工业现场总线的内容和应用实例，因此更名为《可编程序控制器与工业现场总线》。

本书新增加的1章（第4章）是“梯形图编程语言指令系统介绍”，在原书中顾虑该部分内容篇幅较大，希望读者另外从西门子公司的参考手册中去学习这部分内容，因此把这部分省略。后来在实际教学中发现，作为设备维修人员，不了解这部分内容就很难读懂和了解设备供应商开发的程序（尤其对进口设备供应商提供的程序），对于设计和编程人员，熟悉掌握这部分内容也非常重要和有用，所以在新书中增加了完整的1章，这1章也可作为参考手册使用，书末附录中还有指令系统索引表，以备读者随时查阅。

对原书第3章的内容也作了新的补充，这1章补充的内容有OB组织方块的介绍，多背景数据块的概念以及有关GSD文件的说明和如何应用GSD文件在硬件组态目录库中，增加新的器件单元，特别是应用STEP 7软件对第三方产品在分布式I/O系统中的组态等。这些内容是针对学员经常提出的问题加以补充的。

对原书的第5章“现场总线技术”也做了比较大的修改和增加了很多内容，主要是PROFIBUS-DP标准的扩展，在原书中只介绍了DP_V0，现在标准已经扩展到DP_V1和DP_V2，在新书中增加了这部分内容，此外新书还增加了IEC 61158标准中第10类现场总线PROFINET的基本知识。在这1章中花费了比较多的篇幅，对原书现场总线的一个通信实例，进行了彻底改写，改写的例子是S7-300（或S7-400）PLC与Lenze公司新一代传动系统9400的通信程序（DP_94V10项目），对程序的FC 30、FC 127和DB 31做了详细说明，为了便于读者读懂程序，还对STEP 7中的数据结构概念和指针寻址的概念作了详细介绍，新例中除了对参数通道的通信作了详细叙述之外，对过程数据通道通信中涉及传动装置内部的组态，与PLC组态之间的呼应，也作了详细说明，该新例中还包含支持PROFIdrive行规DP_V1协议（参数通道非周期通信）的应用程序（DP_94V10项目中的PZD + DP-V1站）。这一实例程序非常有用，读者掌握这部分内容后，可以直接应用到类似的工程项目中去，对通信实例进行如此详细的分析和解读，在迄今的同类

著作中，还很少见到。这一实例中使用的通信模板型号是 E94AYCPM，适用于 Lenze 9400 伺服控制系统的 PROFIBUS-DP 通信，在原书的例子中用的通信模板是 2133 IB（适用于 Lenze 93 系列和 ECS 伺服控制系统的 PROFIBUS-DP 通信），本书附配套光盘的“Example of this book”文件夹中还保留了原书的这个例子（Exp_S7_），以便需要了解这一实例的读者参考。本书附配套光盘的 Acrobat files 文件夹中列出了这些实例程序的 .pdf 文件，这样即使没有安装 STEP 7 软件，读者也能阅读这些程序文件。

对原书的第 4 章、第 6 章和第 7 章没有再包含在本书中（主要是为了减少篇幅，使全书更为紧凑），对这部分内容有需求的读者在《可编程序控制器与工业自动化系统》一书中仍然能得到，今后著者有机会还会对这部分内容进行更新和补充。

通过新书的出版，著者深信将对读者会有更多帮助。同时也感谢《可编程序控制器与工业自动化系统》一书的读者提出的不少改进意见和期待。

最后，特别感谢唐济扬先生和孙慧民先生为本书所作的序言，唐先生是“中国 PROFIBUS 用户组织”（简称 CPO）的主席，孙先生是“中国 PROFIBUS 技术资格中心”主任，他们二位为“现场总线技术”在国内的开发、应用，标准的制定，产品的测试认证作出了重要贡献，并定期参加相关国际会议和各种技术交流，与国内外同行保持着密切的交往和联系。近年来国内在这一技术领域逐渐接近甚至赶上国际先进水平，这和他们的辛勤工作是密不可分的。唐先生和孙先生在序言中介绍了现场总线技术在国内外的最新发展和动向，也介绍了北京测试认证中心的情况和为用户提供的服务，这些对本书的读者也十分有帮助。在此，代表广大读者再次对唐济扬先生和孙慧民先生表示由衷的感谢！

陈忠华

2010 年 4 月于北京

目 录

序言 1

序言 2

前言

第 1 章 PLC 的发明和发展过程 1

第 2 章 PLC 的定义及硬件和软件的

基本构成 4

2.1 PLC 的硬件体系 4

2.1.1 硬件结构 4

2.1.2 CPU 和中央存储器 6

2.1.3 I/O 接口 9

2.1.4 PLC 的工作原理 21

2.2 PLC 的软件体系 26

第 3 章 PLC 编程语言的应用 28

3.1 西门子公司 S7 PLC 和 STEP 7 编程 软件的应用 28

3.2 西门子公司 STEP 7 编程软件的安装 ... 29

3.3 启动 SIMATIC 管理器 30

3.4 应用 STEP 7 对 PLC 进行硬件组态 31

3.5 S7 PLC 分布式 I/O 模板的组态 37

3.6 应用符号地址编程 43

3.7 STEP 7 的模块化程序结构——组织 方块 OB1 的作用和程序编写 45

3.8 用功能块和数据块建立一个程序 56

3.9 生成功能块 (FB) 的背景数据块及 使用实际参数替代形式参数改变 实际值 61

3.10 使用梯形图逻辑语言编写方块 调用程序 63

3.11 STEP 7 语言中的功能 (FC) 编程 64

3.12 STEP 7 语言中的共享数据块编程 68

3.13 高级功能块和多背景数据块 70

3.14 如何在分布式系统中对第三方产品 进行硬件组态 73

3.15 下载和调试程序 76

3.16 通过监视程序状态的方法来测试 程序 78

3.17 通过建立变量表的方法来测试程序 ... 80

3.18 通过 CPU 诊断缓冲区检查错误 82

3.19 STEP 7 中的组织方块 OB 84

第 4 章 梯形图编程语言指令系统

介绍 94

4.1 STEP 7 梯形图指令系统分类 95

4.2 位逻辑指令类 95

4.2.1 常开触点 (地址) 96

4.2.2 常闭触点 (地址) 97

4.2.3 异或指令 98

4.2.4 取反指令 99

4.2.5 输出线圈 99

4.2.6 中间线输出指令 100

4.2.7 复位线圈 101

4.2.8 置位线圈 102

4.2.9 复位-置位触发器 103

4.2.10 置位-复位触发器 105

4.2.11 RLO 下降沿检测指令 106

4.2.12 RLO 上升沿检测指令 107

4.2.13 保存 RLO 到状态位 BR 指令 108

4.2.14 地址下降沿检测指令 109

4.2.15 地址上升沿检测指令 110

4.2.16 立即读指令 111

4.2.17 立即写指令 112

4.3 比较指令类 112

4.3.1 整型数比较指令 113

4.3.2 双整型数比较指令 114

4.3.3 实数 (浮点数) 比较指令 115

4.4 转换指令类 115

4.4.1 BCD_I 116

4.4.2 I_BCD 117

4.4.3 I_DINT 118

4.4.4 BCD_DI 118

4.4.5 DI_BCD 119

4.4.6 DI_REAL 120

4.4.7 INV_I 121

4.4.8 INV_DI 122

4.4.9	NEG_I	122	指令	155	
4.4.10	NEG_DI	123	4.9.10	取浮点数的自然对数运算 指令	156
4.4.11	NEG_R	124	4.9.11	求正弦函数值指令	156
4.4.12	ROUND	125	4.9.12	求余弦函数值指令	157
4.4.13	TRUNC	126	4.9.13	求正切函数值指令	158
4.4.14	CEIL	126	4.9.14	求反正弦函数值指令	158
4.4.15	FLOOR	127	4.9.15	求反余弦函数值指令	159
4.5	计数器指令类	128	4.9.16	求反正切函数值指令	159
4.5.1	S_CUD	129	4.10	赋值指令类	160
4.5.2	S_CU	130	4.11	程序控制指令类	162
4.5.3	S_CD	132	4.11.1	—(CALL) 指令	162
4.5.4	置计数器值指令	133	4.11.2	用指令框调用 FB 指令	163
4.5.5	加法计数器线圈	134	4.11.3	用指令框调用 FC 指令	164
4.5.6	减法计数器线圈	134	4.11.4	用指令框调用 SFB 指令	166
4.6	数据块指令类: DB 或 DI 指令	135	4.11.5	用指令框调用 SFC 指令	167
4.7	逻辑控制指令类	136	4.11.6	用指令框调用多背景数据块 指令	169
4.7.1	无条件跳转指令	137	4.11.7	从程序库调用方块指令	169
4.7.2	有条件跳转指令	137	4.11.8	使用 MCR (主控继电器) 功能 的重要注意事项	169
4.7.3	遇“非”跳转指令	138	4.11.9	接通主控继电器指令	170
4.7.4	标号	139	4.11.10	断开主控继电器指令	171
4.8	整型数算术运算指令类	139	4.11.11	激活主控继电器指令	172
4.8.1	整型数算术运算指令对状态 字位影响的评估	140	4.11.12	结束主控继电器指令	173
4.8.2	整型数加法运算指令	141	4.11.13	返回指令	174
4.8.3	整型数减法运算指令	142	4.12	移位和旋转指令类	175
4.8.4	整型数乘法运算指令	142	4.12.1	移位指令	175
4.8.5	整型数除法运算指令	143	4.12.2	整型数右移指令	175
4.8.6	双整型数加法运算指令	144	4.12.3	双整型数右移指令	177
4.8.7	双整型数减法运算指令	145	4.12.4	字左移指令	178
4.8.8	双整型数乘法运算指令	146	4.12.5	字右移指令	179
4.8.9	双整型数除法运算指令	147	4.12.6	双字左移指令	180
4.8.10	双整型数除法输出余数指令	148	4.12.7	双字右移指令	181
4.9	浮点数算术运算指令类	149	4.12.8	旋转指令	182
4.9.1	浮点数算术运算指令对状态 字位影响的评估	149	4.12.9	双字左旋转指令	182
4.9.2	实数加法运算指令	150	4.12.10	双字右旋转指令	183
4.9.3	实数减法运算指令	151	4.13	状态位指令类	185
4.9.4	实数乘法运算指令	152	4.13.1	溢出故障位指令	185
4.9.5	实数除法运算指令	153	4.13.2	锁存溢出故障位指令	186
4.9.6	取浮点数的绝对值指令	153	4.13.3	无序故障位指令	187
4.9.7	浮点数二次方运算指令	154	4.13.4	BR 结果位指令	188
4.9.8	浮点数开方运算指令	155	4.13.5	结果位等于 0 指令	188
4.9.9	以 e 为基数的浮点数指数运算				

4.13.6 结果位不等于0指令	189	5.2.2 国际标准的形成过程及现状	221
4.13.7 结果位大于0指令	190	5.2.3 国内发展现状	223
4.13.8 结果位小于0指令	191	5.3 PROFIBUS 现场总线标准介绍	224
4.13.9 结果位大于等于0指令	191	5.3.1 PROFIBUS 标准概念	224
4.13.10 结果位小于等于0指令	192	5.3.2 PROFIBUS 第1层、第2层和 应用层介绍	226
4.14 定时器指令类	193	5.3.3 DP 通信协议	238
4.14.1 脉冲S5定时器	196	5.3.3.1 基本功能 DP_V0	239
4.14.2 扩展脉冲S5定时器	197	5.3.3.2 DP_V1 版本	243
4.14.3 接通延时S5定时器	198	5.3.3.3 DP_V2 版本	245
4.14.4 接通延时保持S5定时器	199	5.3.3.4 用槽号和变址号寻址	247
4.14.5 断开延时S5定时器	200	5.3.3.5 DP 行规	247
4.14.6 脉冲定时器线圈	201	5.3.4 使用 PROFIBUS-DP 进行数据 通信的实例	248
4.14.7 扩展脉冲定时器线圈	203	5.3.4.1 一般描述	248
4.14.8 接通延时定时器线圈	203	5.3.4.2 安装S7程序和方块	250
4.14.9 接通延时保持定时器线圈	204	5.3.4.3 功能说明	258
4.14.10 断开延时定时器线圈	205	5.4 PROFINET 现场总线的基本知识	286
4.15 字逻辑指令类	206	5.4.1 概述	286
4.15.1 WAND_W 指令	206	5.4.2 以太网的MAC地址	288
4.15.2 WOR_W 指令	207	5.4.3 标准以太网的报文帧结构	288
4.15.3 WAND_DW 指令	208	5.4.4 以太网的IP地址	289
4.15.4 WOR_DW 指令	209	5.4.5 有源网络部件	291
4.15.5 WXOR_W 指令	210	5.4.5.1 交换机和集线器	291
4.15.6 WXOR_DW 指令	210	5.4.5.2 路由器	292
4.16 指令系统应用举例	211	5.4.6 基于以太网的通信协议	293
4.16.1 应用定时器指令产生脉冲 序列举例	211	5.4.6.1 TCP/IP	293
4.16.2 模拟量输入模板读程序举例	214	5.4.6.2 UDP/IP	294
第5章 现场总线技术	219	5.4.6.3 ARP 和 RARP	294
5.1 现场总线技术概述	219	5.4.7 以太网报文中的TCP/IP数据	294
5.1.1 现场总线技术产生的背景	219	5.4.8 PROFINET 的网络拓扑结构	296
5.1.2 现场总线技术的概念	220	附录 梯形图指令系统索引表	298
5.2 国内外发展状况	221	参考文献	302
5.2.1 国外发展状况概述	221		

第 1 章 PLC 的发明和发展过程

PLC（可编程序控制器）是 20 世纪 60 年代发展起来的一种新型自动化控制装置。它最早是用于替代传统的继电器控制装置，只有逻辑运算、计时、计数以及顺序控制等功能，而且只能进行开关量控制。因此，其英文原名为 Programmable Logic Controller，简称 PLC，中文名为“可编程序逻辑控制器”。随着技术的进步，其控制功能已经远远超出逻辑控制的范畴，其名称相应改为 Programmable Controller，简称 PC。但 PC 又容易与个人计算机（Personal Computer）的简称 PC 产生混淆，所以近年来人们又倾向于使用 PLC 这一简称，中文名称仍然为“可编程序控制器”。

20 世纪 60 年代，由于美国汽车工业需要进行大规模的技术改造和设备更新，由传统的继电器控制装置进行控制，不仅体积庞大、故障率高、柔性差而不灵活、耗能，而且调试困难，可靠性也差。1968 年由美国通用汽车公司提出使用新一代控制器的设想。从用户的角度考虑，该公司对新一代控制器提了 10 点要求，从而为各大公司提供了明确的开发目标。次年，美国 DEC（数字设备公司）首先研制成功第一台可编程序逻辑控制器 PDP—14。差不多同时，美国 MODICON 公司也研制出 084 控制器。它们的问世，引起了全世界的瞩目，美国的其他公司和西欧、日本等，也相继研究开发出类似的产品。

由于 PLC 不断吸取微电子技术和计算机技术的最新成果，因此发展十分迅速，从单机自动化到整条生产线的自动化，乃至整个工厂的生产自动化，从柔性制造系统、工业机器人到大型分散型控制系统，PLC 均担当着重要角色。

PLC 技术代表了当今电气程序控制的最先进水平。通过 PLC 与各种单元自动化装置（例如智能仪表、数字化传动装置、智能的液压和气动阀组等）以及现场总线、计算机网络系统，构成了车间和工厂自动化的完整体系。

PLC 应用非常广泛。通过近年来对国内进行的调查，得出其在各个领域应用分布大致如下：

• 钢铁和有色冶金	35%
• 汽车和机械制造	20%
• 轻工、食品、包装、造纸	16%
• 化工、石油、工艺过程	13%
• 交通运输、矿山	7%
• 能源、电站、泵站、水处理	7%
• 科研试验、教学	2%

PLC 发明之前，在工业控制的顺序控制领域内，常采用诸如继电器、鼓式开关、纸带阅读器机械，电气元器件作为控制元件，尤其是控制继电器，在离散制造过程控制领域内，成为“开关控制系统”中最广泛使用的元件。但是，随着工业现代化的发展，生产规模越来越大，劳动生产率及产品质量的要求在不断提高，对于控制系统的可靠性也提出了更高的要求，原有“继电器控制系统”已不适应应用需要，究其原因如下：

- 动作缓慢;
- 寿命短、可靠性差;
- 体积大、耗电多;
- 设计制造周期长、程序修改费时;
- 不能实现人-机对话。

到了 20 世纪 60 年代后期,虽然小型计算机已日趋完善,应用领域也在不断扩大,但将小型计算机用于开关控制系统,又显然存在着“大马拉小车”的状态,这是由于小型计算机具有以下特点:

- 编程复杂,要求有较高水平的编程人员和操作人员;
- 需要配套非标准的外部接口,对环境和现场条件的要求过高;
- 功能过剩,机器资源未能充分利用;
- 造价高昂。

基于这种需要与可能,促使人们寻求新的出路,PLC 应运而生。它首先应用于美国汽车工业领域,其中 PLC 部分采用固态(集成)电路来代替继电器逻辑电路,用存储器电路中的存储数位(程序)来代替继电器系统的布线,以程序来规定逻辑关系;用固态 I/O 电路来检测按钮和限位开关的信号,并给出输出以控制电机和其他执行机构。这一阶段的 PLC 系统已开始具有如下一些特点:

- 环境适应性较强,可以使用于车间现场;
- 有较高的可靠性和诊断能力,维修容易;
- 基本能适应不同的制造过程所需,柔性度有了较大提高,只要改变系统中的程序即可改变控制“逻辑”,而无需改造或更换控制硬件等。

自 1976 年以来,开始将微处理器引入 PLC 领域,从而大大加强了 PLC 的作用,使 PLC 由简单地代替继电器电路,而发展为先进的控制装置。当今 PLC 具有采集与处理大量数据、完成数学运算、与其他智能器件通信的能力,并具有先进的人-机对话手段(如操作员面板、SCADA 上位计算机监控和数据采集系统),近年来由于现场总线理念的出现和相关标准的建立,以及产品的迅速发展,PLC 成为现场总线的一个重要组成部分,这进一步扩大了 PLC 的应用领域。

由于 PLC 同时提高了功能和柔性度,使其应用迅速增长,并普及到许多其他离散部件制造工业领域。随后又扩展到批量生产和连续生产过程相关工业领域。随着计算机集成制造系统的发展,PLC 当前还被人们用于工厂通信网络之中,与其他智能控制器和计算机系统一起,成为计算机综合控制系统中的重要组成部分,特别在单元级和工作站级系统中占有重要地位。

从 1969 年第一台 PLC 问世至今,大约经历了 3 个阶段:

第一阶段:所开发的 PLC 容量较小,I/O 点数小于 120 点。用户存储区容量在 2KB 左右,扫描速度为 20 ~ 50ms/KB,指令较为简单,只有逻辑运算、定时、计数等功能,编程语言采用简单的语句表语言,使用上主要用作开关量控制。

第二阶段:PLC 的容量有所扩展,I/O 点数达到 512 点 ~ 1024 点,用户程序存储区扩展到 8KB 以上,速度也有提高,扫描速度达到 5 ~ 6ms/KB,指令功能除了基本的逻辑运算、定时和计数外,还增加了算术运算指令、比较指令及模拟量处理指令等,输入/输出类型也

由纯开关量 I/O, 扩展为带模拟量的 I/O; 编程语言除了使用语句表外, 还可以使用梯形图编程语言。

第三阶段: 进入 20 世纪 80 年代以来, 随着大规模和超大规模集成电路等微电子技术的迅猛发展, 以 16 位和 32 位微处理器构成的 PLC 得到了惊人的发展, 其功能远远超出了上述两个阶段的产品。使 PLC 在概念, 设计, 性能/价格比以及应用方面都有了新的突破。这一阶段的产品向大型和小型两个方向发展。大型产品的 I/O 点数超出 4000 点, 有些产品超过 8000 点, 用户存储区容量达到兆级 (MB)、千兆级 (GB), 并配置有各种智能模块 (例如温度控制模块, 轴定位模块, 过程控制模块等) 和通信模块, 扫描速度也大大提高, 达到 0.47ms/KB 或更高, 指令功能除了基本的逻辑运算、定时、计数、顺序控制外, 还有算术浮点运算指令、PID 调节功能指令、图形组态功能指令、网络和通信指令等; 编程语言普遍采用梯形图语言, 同时也使用语句表和顺序功能图语言 (典型的有 GRAFCET 语言)。为了提高系统的可靠性, 设计上考虑了容错技术和冗余技术等。这一阶段的小型产品向超小型化和加强型功能发展, 有 16 点 I/O 和 24 点 I/O 的整体型小型 PLC, 在小型 PLC 上配置模拟量 I/O, 通信口, 高速计数, 指令上也设置有算术运算、比较指令以及 PID 调节指令。小型 PLC 使用的手握式编程器使用大面积液晶显示器, 也可以用梯形图和 GRAFCET 语言进行编程。

这一阶段 PLC 的软件设计也有很大改进, 普遍实现了软件模块化设计, 在 PLC 产品上提供大量的通用和专用软件功能模块, 用户通过简单的功能调用就可实现复杂的控制任务, 给使用带来极大的方便。使用的编程器越来越完善, 专用编程器实际上已经是一台个人计算机, 可以实现离线编程或在线编程及监控、程序打印以及程序固化, 实现图形组态, 可以联网 (即挂在 PLC 网络上)。有些编程器还可以使用高级语言。除了专用编程器外, 很多 PLC 可以使用通用的笔记本电脑实现编程, 开发一些专用软件, 充分利用个人计算机的能力, 完成各种高级编程功能, 从而省去了专用编程器, 这样既便于推广又节省投资。随着技术的进步, PLC 的功能越来越强, 应用范围越来越广, 与其他工业控制机, 例如集散控制系统 (DCS) 的界限已经不十分明显, 很多以往必须由集散控制系统来完成的控制, 现在用 PLC 都能实现, 因此在应用上 “交错” 已经成为普遍现象。

第2章 PLC 的定义及硬件和软件的基本构成

根据 IEC 标准, PLC 定义如下: PLC 是在工业环境中使用数字操作的电子系统, 它使用可编程序存储器内部存储用户设计的指令, 这些指令用来实现特殊的功能, 如逻辑运算、顺序操作、定时、计数以及算术运算和通过数字或模拟输入/输出来控制各种类型的机械或过程。不论是 PLC 还是与它有关的外部设备都设计成容易集成在一个工业控制系统内, 并容易应用所有计划中的功能。由上述的 PLC 定义, 可以概括 PLC 的特点如下:

1) 控制程序可变, 具有很好的柔性, 在生产工艺流程改变或生产设备更新的情况下, 不必改变 PLC 的硬设备, 只需改变程序就可满足要求。因此, 除单机控制外, PLC 在柔性制造单元 (FMC)、柔性制造系统 (FMS), 以致工厂自动化中也被大量采用。

2) 具有高度可靠性, 适用于工业环境, PLC 产品的平均故障间隔时间一般可达到 5 年以上, 因此是一种高度可靠的工业产品, 大大提高了生产设备的运行效率。PLC 不要求专用设备的机房, 这为工业现场的大量直接使用提供了方便。

3) 功能完善。现代 PLC 具有数字和模拟量输入/输出、逻辑和算术运算、定时、计数、顺序控制、PID 调节、各种智能模块、远程 I/O 模块、通信、人-机对话、自诊断、记录和图形显示、组态等功能。除了适用于离散型开关量控制系统外, 现在也能应用于连续的流程控制系统, 从而使设备的控制水平大大提高。

4) 易于掌握, 便于维修。由于 PLC 使用编程器进行编程和监控, 使用人员只需掌握工程上通用的梯形图语言 (或语句表、流程图) 就可进行用户程序的编制和测试。因此, 即使不太懂得计算机的操作人员, 也能掌握和使用 PLC。也由于 PLC 有完善的自诊断功能, 输入/输出均有明显的指示, 在线监控软件的功能很强, 因此很容易进行维修, 能很快查找出故障的原因。PLC 本身的高可靠性也保证了故障的几率是很低的。

5) 体积小, 省电。与传统的控制系统相比, PLC 的体积很小, 一台收录机一样大小的 PLC 具有相当于 3 个 1.8m 高继电器控制柜的功能。PLC 消耗的功能只是传统控制系统的 $1/3 \sim 1/2$ 。

6) 价格低廉。随着集成电路芯片功能的提高和价格的降低, PLC 硬件的价格也在一直不断地下降。根据最近的市场统计, 国外小型 PLC 平均每一个 I/O 点为 14 ~ 20 美元, 中型 PLC 折算每个 I/O 点为 20 ~ 35 美元, 大型 PLC 折算每个 I/O 点为 40 ~ 80 美元。虽然 PLC 的软件价格在系统中所占的比重在不断提高, 但由于缩短了整个工程项目的设计, 编程和投运费用以及缩短了整个投运周期, 因此, 使用 PLC 的总造价是低廉的, 而且还呈不断下降的趋势。

2.1 PLC 的硬件体系

2.1.1 硬件结构

图 2-1 所示为 PLC 及其与外部设备的联系框图。