

● 现代工业自动化技术应用丛书

现代可编程序控制器 网络通信技术

王仁祥 王小曼 编著



中国电力出版社

www.cepp.com.cn

现代工业自动化技术应用丛书

现代可编程序控制器 网络通信技术

王仁祥 王小曼 编著



中国电力出版社
www.cepp.com.cn



内 容 提 要

本书针对 IEC 61131 可编程序控制器国际标准详细地介绍了现代可编程序控制器的基本结构原理、功能特性; IEC 61131 可编程序控制器国际标准的基本内容及编程语言; 可编程序控制器数据通信、串行通信、网络通信技术原理及 IEEE 802 等网络通信协议国际标准; 工业网络及可编程序控制器网络通信的基本结构原理及应用技术; 现场总线技术基础知识及应用技术, 其中包括 IEC 61158 现场总线国际标准定义的 8 种现场总线, 及目前广泛应用的其他现场总线技术。详细介绍了西门子、三菱的最新可编程序控制器网络结构及网络通信的技术特征、主要技术特点及应用, 并介绍了企业信息网的基本结构及集成技术。书中较多地引用了相关国际标准, 并列举了一些应用实例, 例证了可编程序控制器网络通信及组网技术等。全书密切联系实际, 侧重于实际工程应用。

本书可供从事电气工程自动化、生产过程自动化、工业网络控制技术各领域的工程技术人员阅读及作培训教材, 亦可作为高等学校相关专业的选修课教材和教学参考书, 中等院校相关专业也可选用。

图书在版编目 (CIP) 数据

现代可编程序控制器网络通信技术 / 王仁祥, 王小曼编著.
—北京: 中国电力出版社, 2006

(现代工业自动化技术应用丛书)

ISBN 7-5083-4144-9

I. 现... II. ①王...②王... III. 可编程序控制器—应用—通信网 IV. ①TP332.3②TN915

中国版本图书馆 CIP 数据核字 (2006) 第 013810 号

中国电力出版社出版、发行

(北京三里河路 6 号 100044 <http://www.cepp.com.cn>)

北京丰源印刷厂印刷

各地新华书店经售

*

2006 年 5 月第一版 2006 年 5 月北京第一次印刷

1000 毫米×1400 毫米 B5 开本 28.25 印张 578 千字

印数 0001—4000 册 定价 44.00 元

版 权 专 有 翻 印 必 究

(本书如有印装质量问题, 我社发行部负责退换)

序 言



现代工业自动化技术是信息社会中的关键技术和核心技术之一。自动化技术促进了人类文明的发展。实现工业生产自动化可以提高系统性能、改善劳动条件、减轻劳动强度、大幅提高生产率、节约能源、提高产品质量和经济效益。自动化设备可以代替人完成各类高危作业。

现代工业自动化系统已呈现开放性、智能化、信息化与网络化的特点，它融合了自动化技术、信息技术、现代控制技术、网络技术、通信技术、先进制造技术及现代管理学等诸多学科的先进技术，需要各学科的专家及工程技术人员通力合作，从而实现多学科专业知识与系统集成、形成实现现代工业自动化发展的手段或模式。

为了推广现代工业自动化技术的应用，总结、发展和提高我国工业自动化技术的应用水平，培养高水平的工程技术人员，帮助工作在生产第一线的工程技术人员能够及时拓展知识结构，较全面地了解和掌握现代工业自动化领域中的最新技术和应用，中国电力出版社组织编写了《现代工业自动化技术应用丛书》。

一、丛书的编写宗旨

团结组织工业自动化领域的专家、学者、科技工作者、工程技术人员和团体，共谋策划与编写，促进我国工业自动化技术的繁荣和发展。

二、丛书的编写原则

1. 以技术应用为主。理论与实践密切结合，通过剖析工程实例，介绍最新技术和产品的应用，以适应工业现场的需要。可操作性强。
2. 丛书各分册均以现场应用实际或范围划分。各分册之间既相互联系又自成体系。
3. 编委会特邀请该领域有扎实理论基础并富有实践经验的专家、学者和工程技术人员来承担编写工作。

三、丛书读者对象

以工程技术人员为主要读者对象，也适宜科研人员和大专院校师生参考。

我们相信《现代工业自动化技术应用丛书》的出版必将对我国工业自动化技术的应用起到积极作用。编写出版《现代工业自动化技术应用丛书》对于我们是一种全新的尝试，难免存在一些问题，希望广大读者给予支持和帮助，我们的联系

方式是 mo_bingying@cepp.com.cn。同时,热忱希望各行业从事工业自动化及相关技术的专家、学者、工程技术人员借此机会积极参与,将您在工作实践中获得的丰富经验总结出来,共同为提高我国工业自动化技术的应用水平做出贡献。

《现代工业自动化技术应用丛书》

编委会

前 言



20 世纪 60 年代后期, 美国汽车制造业根据当时汽车市场需求和计算机技术的发展, 提出以计算机为基础的 Modular Digital Controller (MODICON) 装置控制方案取代生产线上的继电逻辑控制盘, 其核心思想是采用软件编程方法替代硬接线继电逻辑控制方式, 后来 MODICON 公司生产的 MODICON 084 PLC (Programmable Logic Controller) 成为世界上第一种投入商业生产的 PLC, 也是现代 PLC 的原型, 之后, 从 20 世纪 70 年代 PLC 崛起时期开始到 20 世纪 90 年代末期, PLC 逐步走向成熟并进入了快速发展时期, 随着国际标准 IEC 61131 的推广应用, 进入 21 世纪后, 由于现代工业自动化技术的进步, 信息技术、自动控制技术、智能化技术、网络技术及多媒体技术等迅速发展, PLC 技术有了突飞猛进的发展, 在系统体系结构上采用开放的通信接口, 支持面向现场总线网络的体系结构, 从传统的单机控制向多 CPU 和分布式及远程网络化控制系统发展; 在编程语言上支持文本化和图形化多语言编程方式, 创造了更具表达控制要求、文字处理、通信能力和界面友好的编程环境; 以 PLC 为基础的系统应用不断拓展, 全方位地提高了 PLC 的应用范围和水平, 趋向于建立同一硬件平台, 运用同一个操作系统、同一个编程系统, 执行不同的 PLC 功能, 以实现 EIC 三电一体化。新型 PLC 可在一个机架上装插多个 CPU 模块, 可将 PC 机模块与 PLC 的 CPU 模块、过程控制 CPU 模块或运动控制模块同时插在一个机架上, 使 PLC 系统可直接与生产管理计算机系统集成成为两层通信结构, 构成快捷方便的工业自动化网络化控制系统, 实现从工业机器人到智能机器人、网络机器人的开发与应用, 从工业总线到现场总线再到工业以太网的相互关联与渗透等, 可使工业控制系统的结构、运动、检测、控制、驱动充分融合与集成, 自动化系统的信息化、数字化、智能化、网络化进一步提高。本书就是基于上述技术发展的背景而编写的。

本书编排特点是并不拘泥于某种型号的 PLC 及其具体细节, 而是基于 IEC 61131 国际标准详细地介绍现代可编程序控制器的基本结构原理、功能特性, 从 PLC 的共性特征出发介绍 PLC 的基本原理、结构、功能及使用等方面的知识, 重点介绍了 IEC 61131 可编程序控制器国际标准的基本内容及编程语言, 同时也介绍了现代可编程序控制器的基本技术细节; 可编程序控制器数据通信、串行通信、网络通信技术原理及 IEEE 802 等网络通信协议国际标准; 工业网络及可编程序控制器网络通信的基本结构原理及应用技术; 现场总线技术基础知识及应用技术, 其中包括 IEC 61158 现场总线国际标准定义的 8 种现场总线, 及目前广泛应用的其他现场总线技术。详细介绍了西门子、三菱的最新可编程序控制器网络结构及网络通信

的技术特征、主要技术特点及应用,并介绍了企业信息网的基本结构及集成技术。书中较多地引用了相关国际标准,并列举了一些应用实例,例证了可编程序控制器网络通信及组网技术等。全书密切联系实际,侧重于实际工程应用。

全书共5章及绪论组成,绪论中概述了现代PLC和现场总线技术的发展概况;第1章介绍了PLC共性的基本知识;第2章介绍了IEC 61131可编程序控制器标准及编程语言及现代可编程序控制器的基本结构原理;第3章介绍了可编程序控制器网络通信与现场总线技术基础知识与技术特征;第4章详细介绍了西门子、三菱的最新可编程序控制器网络结构及网络通信系统;第5章介绍了工业自动化网络化控制系统集成的基本知识和方法。各章节中均有相应的应用实例。本书从PLC和现场总线应用系统的角度介绍基本原理,然后通过应用系统实例进一步叙述技术特点,使读者能系统了解和掌握PLC及其网络系统和现场总线系统的技术细节。书中第2~4章的主要内容较多地取材于外文原文资料,结合工程实际编写而成,王小曼承担了部分外文资料初译工作,并编写了第1章和第2章的数据通信部分、绘制了书中插图。本书编写过程中曾参考和引用了国内外许多厂商、专家与学者发表的论文与著作,以及一些产品的说明书,由于各种因素不能一一预告、面谢,作者在此一并致谢。本书具有内容新颖、起点高、系统性和实用性特点,可供从事电气工程自动化、生产过程自动化、工业网络控制技术各领域的工程技术人员阅读及作培训教材,亦可作为高等学校有关专业的选修课教材和教学参考书,中等院校相关专业也可选用。

由于作者水平及时间所限,书中难免存在不妥、缺点和谬误,热忱欢迎广大读者批评指正,将不胜感谢。

编 者

目 录



序言	
前言	
绪论	1

第1章 可编程序控制器概述 8

1.1 可编程序控制器的发展 8

1.1.1 可编程序控制器的发展历程	8
--------------------	---

1.1.2 我国可编程序控制器的发展	12
--------------------	----

1.1.3 可编程序控制器的最新发展和趋势	13
-----------------------	----

1.1.4 可编程序控制器编程软件的发展	16
----------------------	----

1.1.5 可编程控制器网络控制技术的发展	19
-----------------------	----

1.2 可编程序控制器的原理 24

1.2.1 可编程序控制器的硬件结构原理	25
----------------------	----

1.2.2 可编程序控制器的软件系统	34
--------------------	----

1.2.3 可编程序控制器的工作原理	36
--------------------	----

1.3 可编程序控制器的编程语言与编程软件 44

1.3.1 梯形图 (LD) 程序设计语言	45
-----------------------	----

1.3.2 指令列表 (IL) 程序设计语言	48
------------------------	----

1.3.3 顺序功能图 (SFC) 程序设计语言	54
--------------------------	----

1.3.4 编程环境简介	63
--------------	----

第2章 IEC 61131 可编程序控制器标准简介 69

2.1 IEC 61131 标准概览 69

2.2 可编程序控制器的基本功能结构和特征	72
-----------------------	----

2.3 IEC 61131-3 标准简介 73

2.3.1 5种编程语言及其相互关系	73
--------------------	----

2.3.2 IEC 61131-3 标准的主要特点	75
---------------------------	----

2.3.3 IEC 61131-3 标准的软件模型、通信模型和编程模型	77
-------------------------------------	----

2.4 IEC 61131-3 标准编程语言简介 109

2.4.1 功能块图语言 (FBD)	110
--------------------	-----

2.4.2 结构化文本语言 (ST)	117
--------------------	-----

第3章 可编程序控制器网络通信与现场总线技术基础 125

3.1 概述 125

3.1.1 可编程序控制器网络	125
-----------------	-----

3.1.2 现场总线技术	127
--------------	-----

3.1.3 工业企业网	137
-------------	-----

3.2 数据通信与网络协议基础 141

3.2.1 数据编码	142
------------	-----

3.2.2 数据通信的基本概念和技术指标	144
----------------------	-----

3.2.3 数据通信方式	148
--------------	-----

3.2.4 网络通信协议	149
--------------	-----

3.2.5	介质访问控制	183
3.2.6	通道利用方式	188
3.2.7	网络拓扑结构	189
3.2.8	通信传输介质	191
3.3	串行通信基础	196
3.3.1	概述	196
3.3.2	RS232C 串行通信接口	200
3.3.3	RS423 串行通信接口	205
3.3.4	RS422 串行通信接口	205
3.3.5	RS485 串行通信接口	206
3.3.6	串行通信编程方法	210
3.3.7	USB 总线接口	211
3.3.8	蓝牙技术简介	214
3.4	可编程序控制器网络通信基础	216
3.4.1	全局 CIMS	217
3.4.2	可编程序控制器网络通信的功能特点	220
3.4.3	可编程序控制器网络中的通信方式	230
3.4.4	工业计算机标准 Compact PCI	233
3.5	现场总线技术基础	237
3.5.1	现场总线通信协议模型	238
3.5.2	现场总线控制系统的体系结构	241
3.5.3	现场总线控制系统的组成	243
3.5.4	现场总线控制系统的拓扑结构	246
3.5.5	现场总线控制系统的类型	248
3.5.6	其他现场总线控制系统的类型	273
3.5.7	现场总线网络硬件与现场总线产品	286

第4章 可编程序控制器网络通信

.....	288
4.1 概述	288
4.2 可编程序控制器通信网络中常用的通信方式	289
4.2.1 可编程序控制器控制网络中常用的通信方式	290
4.2.2 分层结构工业控制网络的建立	290
4.2.3 以现场总线为基础的工业企业网结构	293
4.3 西门子可编程序控制器网络通信	296
4.3.1 西门子 SIMATIC 技术概述	296
4.3.2 西门子可编程序控制器简介	297
4.3.3 西门子可编程序控制器通信网络概述	315
4.3.4 S7-200 的数据通信网络	319
4.3.5 S7-300 的数据通信网络	335
4.3.6 S7-400 的数据通信网络	357
4.3.7 SIMATIC NET OPC 服务器与 S7 的组态	360
4.4 三菱可编程序控制器网络通信	365
4.4.1 概述	366
4.4.2 MELSEC-Q 系列 PLC 通信网络	375
4.4.3 三菱 PLC 通信网络组网	387

第5章 工业控制网与信息化平台的集成 390

5.1 概述 391

5.2 管理信息系统平台 395

5.2.1 生产计划管理系统 395

5.2.2 生产调度子系统 396

5.2.3 质量管理子系统 397

5.2.4 设备管理子系统 397

5.2.5 物资管理子系统 398

5.2.6 人力资源管理子系统 399

5.2.7 领导决策支持系统 400

5.2.8 销售管理子系统 400

5.2.9 财务管理子系统 401

5.2.10 办公自动化子系统 401

5.2.11 视频监视与监控子系统 ... 403

5.2.12 权限管理子系统 404

5.2.13 数据管理子系统 404

5.3 企业内部网组网与集成 409

5.3.1 企业内部网 409

5.3.2 Intranet 的体系结构 415

5.3.3 网络规划 423

5.3.4 网络的设计和实施步骤 ... 424

5.3.5 网络计算模式 426

5.4 工业组态软件简介 433

主要参考文献 442

绪 论

随着现代工业自动化技术的进步,信息技术、自动控制技术、智能化技术、网络技术及多媒体技术等迅速发展,各种工业网络已渗透到各行各业,基于可编程程序控制器 PLC (Programmable Logic Controller) 控制及其网络的各类工业设备也得到了很大发展,已广泛应用于各行各业。在目前普遍使用的可编程序控制器中,已经具备实时在线通信能力,并可通过上位计算机与现场总线通信网络实现对工业现场设备的实时监测、实时控制,实现多机分布式控制系统。

现代信息技术的普及应用是现代社会的一个显著标志。现代信息技术的核心是计算机和现代通信技术。现代计算机无论在信息量存储,还是信息处理速度方面都在飞速发展,同时,性能大幅度提高,而价格却大幅度下降,这也是计算机广泛应用和社会文明的基础。现代通信技术的迅速发展大大提高了信息传递的速度和通信能力,从而多种信息媒体(数字、声音、图形、图像)的传输使社会状况发生了极其深刻的变化。现代工业自动化就是综合运用了现代信息技术、现代微电子技术、自动控制技术、智能化技术和网络技术等对生产过程实现自动检测、控制、优化、调度、管理和决策的综合性技术。现代工业自动化根据生产过程的特点可分为过程控制自动化、制造工业自动化以及各种自动化测控系统等。

工业生产过程控制系统是一个分散控制系统,最优的控制方式是分散控制、集中监视、操作和管理。工业自动化控制系统通常包括开关量逻辑控制系统、模拟量连续过程控制系统及运动控制系统。这三种控制系统分别采用不同的控制装置来实现,开关量逻辑控制系统传统上采用继电逻辑控制方式实现,目前可编程序控制器在这种系统中扮演着重要角色;模拟量连续过程控制系统传统上采用过程控制仪表如电动单元组合仪表等实现,现在普遍采用的智能化可编程调节器代表着当代先进的控制方式;运动控制系统传统上采用各种电气传动控制装置、伺服控制系统等来实现,目前已被通用变频器控制系统和各种运动控制器所替代。从现代控制技术或装置来看,无论是逻辑控制、过程控制、还是运动控制都引入了计算机控制技术,从而计算机控制技术已成为三种控制系统的核心。而计算机控制技术的重要特征是它的软件丰富、数据处理及通信能力强,这就为网络化控制造就了坚实的基础,在控制网络中,尽管三种系统各不相同,但网络已成为它们相互联系的载体,通过各自的通信功能可连入同一网络,通过现场总线的链接可以实现三种系统的一体化控制,即通常所说的三电一体化。所谓“三电”,在工业自动化控制领域是指电气控

制、过程控制（或仪表控制）和计算机控制系统的三电一体化系统，通常简称 EIC。泛指电气控制装置、工业检测及控制仪表、工业自动控制装置和计算机控制系统的系统集成。在一个自动控制系统中，系统中的检测仪表把各种信息收集起来，通过网络传给系统中的主控计算机，计算机接受信息后，经过计算或判断后向控制系统的执行机构如电气传动装置和控制仪表等发出执行指令执行。这是一个整体，各部分密不可分，往往将其综合在一起，统一考虑其设计、制造、安装、调试，直至投入运行。这个过程称为系统集成，集成形成的产品，称为三电一体化产品，这是自动化控制系统发展的方向，其发展程度代表着当代工业自动化技术水平。

在工业自动化技术发展过程中，不同的工业领域和控制对象各自发展了相应的控制技术和装置，其中具有代表性的装置有可编程序控制器、工业计算机（IPC）和智能化仪器仪表，以及由这些装置集成的控制系统，如集散型控制系统 DCS（Distributed Control System）、可编程序控制器控制系统 PCS、现场总线控制系统 FCS（Fieldbus Control System）和以工业计算机为基础的开放式控制系统等，这些系统在各自的应用领域中均得到了很大发展，使传统工业生产过程发生了划时代的变革，带来了新的活力，使得工业生产技术水平不断提高。这些系统中包含了诸多的先进技术，如先进控制技术、过程优化技术、智能化技术、实时监控技术、信息集成技术、系统集成技术、地理信息技术、现场总线及通信技术等，并日新月异地向前发展。各种控制网络已渗透到各行各业，生产过程自动化系统和生产管理系统被融合在一起，在数据采集、管理、数据和知识共享、硬软件资源共享等方面，特别是在设备控制、过程控制、生产控制之间，形成了管控一体化。现代集成制造系统 CIMS（Contemporary Integrated Manufacturing System）、现代集成制造系统应用网络（CIMSNET）、生产过程优化控制与制造执行系统（MES）、现代企业管理系统（如 ERP、CRM、SCM）、电子商务平台、区域制造网络系统等蓬勃发展，现代工业生产过程正向着网络化制造、综合自动化方向发展，在控制系统中打破了传统的 IPC、PLC、DCS 的分工界限，构成有机组成的三电一体化综合自动化系统。实际上，一个控制系统中往往既有过程控制又有离散控制，因此，一些 PLC 制造商致力于研究开发 PLC 过程控制功能，向融合过程控制和离散控制方向发展，产品具有数字化、模块化和网络化的特点，既可构成性能优异的 DCS 系统，又可灵活地配置各种应用的 PLC 控制系统，能方便地实现三电（EIC）一体化系统，同时也是优秀的管理系统，如 Siemens 公司的 SIMATIC PCS7 就是具有上述特点和功能的全集成、结构完整、功能完善、面向整个生产过程的过程控制系统，其集成的核心是具有统一的过程数据库和唯一的数据库管理软件，所有的系统信息都存储于一个数据库中，而且只需输入一次，从而增强了系统的整体性和信息的准确性。SIMATIC PCS7 采用上位机软件 WinCC 作为操作和监控的人机界面，利用 PROFIBUS 现场总线和工业以太网实现现场信息采集和系统通信，工业以太网用于系统站之间的数据

通信,具有 ODBC、OLE 等标准接口,从而具有很强的开放性,可以方便地连接上位机管理系统和其他厂商的控制系统;以 S7 自动化系统作为现场控制单元实现过程控制;通过分布式 I/O 接收现场传感器的检测信号;采用符合 IEC 61131-3 国际标准的编程软件和现场设备库,提供连续控制、顺序控制及高级编程语言。现场设备库提供了大量的常用现场设备信息及功能块,可大大简化组态工作、缩短工程周期。

分布式网络、过程控制软件和各种应用软件的发展,使得人们可以按照自己的意愿建立一个控制网络,摆脱传统工业化模式,探索信息化途径,从而使得作为工业过程自动化控制核心的工业计算机 IPC、可编程序控制器 PLC 及集散控制系统 DCS,相互渗透,融会贯通,形成了全集成自动化系统。所谓全集成自动化系统就是打破上位机和工业控制器之间,连续控制和逻辑控制之间,集中与分散之间的界限,统一数据管理、统一通信、统一组态和编程软件,用一个多功能系统平台完成原来需要由多种系统才能完成的功能,从而大大简化了系统结构,减少大量接口部件和成本。基于这种多功能系统平台,各种各样不同的技术可以集成在一个具有全局数据库的平台上,技术人员可以对所有应用进行组态、编程和监控,大大提高了系统运行水平。西门子公司的“APACS+过程自动化系统”就是将 DCS 和 PLC 一体化的过程自动化系统,它使用一套软件工具就可将传统上由过程控制系统、可编程序控制器、上位监控计算机、SCADA 系统和人机界面等共同控制的、分离的功能统一起来,为组态、测试、文件化、故障诊断和培训提供一个共同的环境,完全消除了传统的工程设计方法,允许用户在不同的系统之间互换数据,用户可以任意选用不同厂商的产品。所有这些特点的实现,是由于它广泛采用了包括用于可编程序控制器的 IEC 61131-3 标准、用于过程控制的 OLE (OPC)、SQL 数据库管理、工业以太网、动态数据交换 (DDE) 和控件 ActiveX 等工业标准来实现的。

从技术发展上看,系统中基于计算机技术的控制装置越来越多,系统中的设备和装置都在智能化 (Smart 或 Intelligent),全新的工业控制结构是一个装置智能化、管理信息化、控制分散化、网络分散化、完全开放的、模块化体系结构的控制系统。系统中的现场设备已经具备实时在线通信能力,既能分别控制各自的对象,又能相互协调,形成连续自动控制系统,系统中的现场设备可以采用计算机通过现场总线链接,进行网络化控制,计算机与网络上任一现场设备之间可以方便地通信,实现实时监测、实时控制、按预先设定的工作流程和控制策略,实现多机分布式控制系统,而其中的工业计算机和可编程序控制器扮演着重要角色。工业计算机具有能快速、实时、大量处理复杂数学模型和数据、以及总线标准化程度高、兼容性强、软件资源丰富、具有实时操作系统的支持的特点,对于复杂工业控制对象的控制占有优势。近年来,随着微电子技术、大规模集成电路技术、计算机技术和通信技术等的的发展,可编程序控制器在技术和功能上发生了飞跃。在初期逻辑运算的基

础上,增加了数值运算、模拟量控制、PID 调节器和网络控制等功能,运算速度大幅度提高,中央处理器的性能与工业计算机相当,并具有多种局部总线和网络,向下拓展功能,开放总线,因而可方便地构成一个开放式集散控制系统。目前从硬件角度看,PLC、IPC、DCS 之间的差别越来越小,在应用软件方面也有很多相同点。尽管如此,由于 IPC、DCS 和 PLC 属于不同类别的产品,在各自的发展过程中都形成了各自的专用软件和技术特点,短期内还难以统一。但随着开放式工业计算机系统的发展,PLC 和 DCS 的软件系统可与系统硬件分离,形成“Soft PLC (软 PLC)”、“Soft DCS (软 DCS)”和“多功能控制器平台”的应用环境,将软应用环境装载在开放式工业计算机系统平台上,形成以开放式工业控制计算机系统为核心的主控系统,在此基础上可以由第三方根据需要开发实时监控软件平台和信息集成软件平台等。实质上,PLC 的核心就是一台工业环境下应用的计算机,计算机的最大优势就是可以在一个通用平台下运行各种应用软件;而 PLC 的最大优势是在工业环境下应用的可靠性,这种可靠性有赖于专用处理器和本身固化的软件系统及符合其规范的用户程序,这就使得不同品牌 PLC 之间存在着较大差异,开放性受到限制。但随着现代操作系统、微内核设计技术和模块化设计技术的发展,嵌入式系统技术已被引入到 PLC 中,PLC 的硬件可采用嵌入式微处理器,软件将以通用嵌入式实时操作系统为核心,开发环境类似于人们已经熟悉的 UNIX、Windows 等操作系统,应用程序可完全摆脱依赖于专用软件系统的制约。PLC 最常用的编程语言是梯形图语言,新型的产品均已采用了 IEC 61131-3 国际标准程序设计语言,包括梯形图、功能块图表、顺序功能图表、结构化文本和指令表等程序设计语言,用户可以任意选择其中的一种甚至是多种语言混合编程。GE Fanuc 公司的新产品 PACSystems — RX7i、PACSystems — RX3i 系列可编程自动化控制器 PAC (Programmable Automation Controller),就是一种采用通用实时操作系统 VxWorks 及控制引擎 (control engine)、嵌入式硬件系统和背板总线组成的一种全新结构的可编程序控制系统,它具有开放式模块化控制结构,将逻辑控制、运动控制、过程控制和人机界面等功能集成在一个通用开发平台上,可满足多领域开放式自动化控制系统的设计和集成,允许 OEM 厂商和最终用户在这个统一平台上集成多个控制对象的控制。对于不同的硬件平台,PAC 系统提供了一个相同的控制引擎和通用编程软件,用户具有任意选择硬件系统的灵活性,当硬件系统扩展和变化时,用户的系统和程序无需变化,即可无缝移植。

软 PLC 是开放的可编程序控制器,容易连接各种 I/O 模块、功能模块、运动控制模块和网络等,具有丰富的编程指令,操作更加快速和安全,可在实时多任务操作系统、网络控制和分级控制领域广泛应用。以工业计算机为平台的软 PLC 控制系统,是将工业计算机系统与控制软件组合在一起,将 PLC 的控制功能“封装”在软件内,运行于工业计算机中,操作系统可以用 Windows NT 或 Windows CE 等。这样,系统既具有了可编程序控制器功能,又具备了工业计算机的

各种优点,大大简化了工厂自动化的体系结构,还可以充分利用工业计算机日新月异的软硬件发展环境,不断地升级和更新换代。工业计算机技术提供的许多功能,能够增强可编程序控制器的功能特性,包括内藏视频、内藏 Web 和高速浮点数字处理等。但这并不意味着工业计算机控制将取代可编程序控制器控制,工业计算机控制只是可替代可编程序控制器的 CPU 单元,而不能替代它的 I/O 功能。I/O 功能仍然是可编程序控制器原有的或者是由第三方 I/O 生产厂生产的产品,其发展方向必然是运用现场总线、工业控制网络构筑完全开放式分布系统。完全开放式就是在产品设计、装置和器件选择、网络通信、操作系统、监控及显示等方面都采用国际标准或大家公认的工业标准,使不同厂商的产品相互兼容、互换,能被集成在一个网络中运行,通过网络能把一个复杂的控制系统简单化,并生成直观的人机交互界面。

可编程序控制器的通信联网能力是其发展的重要标志。可编程序控制器网络是将可编程序控制器与计算机、可编程序控制器与可编程序控制器、可编程序控制器与其他可通信终端设备连成的通信网络,其发展趋势是实现一种高速、多层次、大容量、高可靠和开放式的控制网络。现场总线可以和可编程序控制器构成廉价的集散控制系统,并具有广泛的全局性、整体性系统集成扩展空间,能方便地实现基本系统的局部扩展、远程扩展以及基本系统的联网,支持多种网络协议,可用双绞线连接实现远程通信。另外,利用 PLC 的 I/O 子系统可实现远程 I/O 就地分散安装,通过现场总线可将现场设备直接连接,集检测、数据处理、通信和设定、调试为一体,能在现场完成智能 I/O 功能,实现现场控制并自诊断,且危险分散,增加了系统的自治性和可靠性。智能型 PLC 的 I/O 子系统是以微处理器、数据存储器及程序为基础的模块化功能部件,具有执行预处理、控制、故障检测、冗余输出和通信等功能,而且不依赖于扫描工作方式,提高了 PLC 的运行和扩展的灵活性。工业以太网(EtherNet)是继现场总线之后发展起来的一种工业控制网络,它已在可编程序控制器控制网络中广泛应用。罗克韦尔自动化公司最近宣布推出标准工业以太网协议 EtherNet/IP,它是标准 TCP/IP 以太网和通用工业协议(CIP)的结合,将标准 TCP/IP 以太网延伸到工业实时控制,更加开放集成的工业自动化和信息化系统。

近年来,可编程序控制器厂商在 RS232/422/485 通信接口的基础上,逐渐增加了各种通信接口和完整的控制网络。可编程序控制器网络已成为具有 3~4 级子网的多级分布式网络,其配置的工具软件,可使它成为具有工艺流程显示、动态画面显示、趋势图生成显示、各类报表制作等的多功能系统,可以方便地与其他网络互联。现在几乎每一品牌产品的通信系统都力图为用户提供开放式的结构和连接,将应用对象、PLC、自动化装置、第三方设备和计算机平台连接起来;将控制、过程、生产信息集成为整体的控制系统。PLC 网络的发展方向是高速、多层次、高可靠性、大吞吐量,并符合国际工业标准的开放性、跨平台的开放体系结构,以实现

最高级的集成。现在,越来越多的 PLC 具有了 EtherNet 接口部件和内藏 Web 服务器,可将 EtherNet 技术应用到工厂底层的现场过程控制设备中。通过内藏 Web 服务器,可将企业内部所有自动化控制设备连接到企业局域网 Intranet 和 Internet 中去,允许现场过程控制器之间共享数据信息,其中,通常采用 OPC 服务器设备驱动程序来连接实时数据信息,利用 EtherNet 网络系统和 Web 技术可以进行远程文件传输、程序设计、参数修改和系统维护。这样,用户不但可在任何地方监控控制系统的运行状况,而且还可以随时获取所需要的数据信息。由于数据通信技术发展很快,现场总线技术及 EtherNet 技术也同步发展,所以可编程序控制器控制系统 PCS 发展迅速。目前罗克韦尔 AB 公司已形成了多层结构体系,即 EtherNet、ControlNet、DeviceNet 及 Asi 等现场总线。西门子公司在 Profibus - DP 通讯网络及 Profibus - FMS 网络以外,提出了 S7 Routing 网络,即 Profibus - DP 和 EtherNet 两层结构。

现场总线控制系统 FCS 是伴随着计算机网络技术的飞速发展而兴起的一种基于现场总线技术的现代计算机控制系统,是集计算机技术、网络技术和控制技术为一体的全分散、全数字、全开放的计算机控制系统和技术,是现代工业过程自动化控制及楼宇自动化等领域中实现计算机控制系统的最先进技术。基于现场总线技术的现场仪表与控制系统之间可实现全分散、全数字化、智能、双向互联、多变量、多点、多站的通信网络系统。具有可靠性高、稳定性好、抗干扰能力强、通信速率快、系统安全、造价低廉、维护成本低等特点。现场总线技术使现场级设备的信息作为整个企业信息网的基础,提高了控制系统的信息处理能力和运行可靠性,节省了系统的硬件和布线费用,方便了用户对系统的组态、管理和维护。现场总线控制系统 FCS 的技术关键是智能执行机构(仪表)技术和现场总线技术,结合计算机和可编程序控制器等的丰富的软硬件资源,克服了传统控制系统的缺点,形成了一种全新的控制系统,是工业自动化控制系统发展的方向。随着计算机控制技术的发展及数据交换技术的完善,基于 EtherNet/IP 的测控系统将会和 FCS 逐步融合在一起,通过现场总线技术,现场设备成为以微处理器为核心的数字化设备,彼此通过传输媒体(双绞线、同轴电缆或光纤)以总线拓扑相连;网络数据通信采用基带方式传输,即数字数据传输,数据传输速率高达 10Mbit/s/100Mbit/s 级,实时性好,抗干扰能力强;系统中的 I/O 控制站分散在网络底层,由通信网络完成,分散的功能模块便于系统维护、管理与扩展,提高可靠性;开放式互连结构,既可与同层网络相连,也可通过网络互连设备与控制级网络或管理信息级网络相连;互操作性,在遵守同一通信协议的前提下,可将不同厂家的现场设备产品统一组态,构成所需要的网络。现场总线通信协议遵照 ISO/OSI 参考模型,主要实现第 1、2、7 层功能。物理层采用 RS232/RS422/RS485 通信接口。数据链路层介质访问控制多采用受控访问协议,通常,由 PC、PLC 作为主站,可通信设备如通用变频器、传感器、变送器、数字 I/O 设备等作为从站,支持点对点、一点对多点和广播通信方

式。应用层解决应用什么样的网络软件包括过程控制语言来作为面向用户的编程或组态语言，其中包括设备名称、网络变量与配置（捆绑）关系，参数与功能调用及相关说明等，一般应具有符合 IEC 61131 国际标准的图形用户界面（GUI）。由此可见，现场总线将现场设备与工业过程控制单元、现场操作站等互连而成的工业控制网络，具有全数字化、分散、双向传输和多分支的特点，是工业控制网络向现场级发展的方向。