XIMENZI PLC

GONGCHENG YINGYONG YU GUZHANG JIANXIU SHILI

西门子PLC

工程应用与故障检修实例

周志敏　纪爱华　等 编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

XIMENZI PLC

GONGCHENG YINGYONG YU GUZHANG JIANXIU SHILI

西门子PLC

工程应用与故障检修实例

周志敏　纪爱华　等 编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书以西门子 PLC 控制系统设计、工程应用及故障处理为核心内容，在简单介绍了西门子 PLC 发展、分类、特性的基础上，系统地介绍了西门子 PLC 控制系统设计要点、西门子 PLC 工程应用实例、PLC 故障诊断及处理方法、西门子 S 系列 PLC 维护及故障处理实例等内容。本书在写作上以理论与工程应用相结合的方式，深入浅出地阐述了西门子 PLC 控制系统设计与工程应用中，经常涉及的设计条件、PLC 选型、设计方法、工程应用实例及故障诊断处理方法。

本书重点突出，实用性强，可供从事西门子 PLC 控制系统设计、工程应用及维修的工程技术人员使用，也可供高等院校及职业技术学院的师生阅读参考。

图书在版编目（CIP）数据

西门子 PLC 工程应用与故障检修实例/周志敏等编著. —北京：中国电力出版社，2016.3

ISBN 978-7-5123-8729-4

Ⅰ.①西… Ⅱ.①周… Ⅲ.①plc 技术-应用②plc 技术-故障修复 Ⅳ.①TM571.6

中国版本图书馆 CIP 数据核字（2016）第 004509 号

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）

北京雁林吉兆印刷有限公司印刷

各地新华书店经售

*

2016 年 3 月第一版 2016 年 3 月北京第一次印刷

787 毫米×1092 毫米 16 开本 13.25 印张 323 千字

印数 0001—3000 册 定价 **33.00** 元

前　言

PLC是电气自动化控制系统的重要组成部分，它自问世以来不断发展和改进，现在已广泛应用于工业企业的各个领域，其性能的优劣直接关系到整个控制系统的安全性和可靠性指标。

学习PLC控制技术，即是学习如何将PLC应用到自动化控制工程实践中，这也是保证由PLC构成的电气自动化控制系统具有高性能比、最佳性能指标的技术基础。而掌握PLC故障诊断及处理方法，则是确保PLC控制系统安全稳定运行的实际操作技能。这两部分知识和技能正是本书主要讲述的内容。

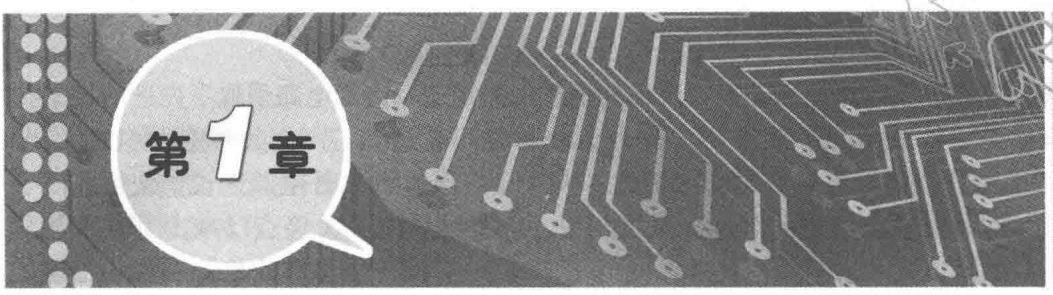
本书结合国内外西门子PLC控制系统的工程应用实践，在简单介绍了西门子PLC特性的基础上，系统地介绍了西门子PLC控制系统设计、工程应用、故障诊断及处理方法。本书在写作上尽量做到有针对性和实用性，力求通俗易懂和结合实际，使得从事PLC控制系统设计、工程应用及维修的工程技术人员从中获益，从而以此为“桥梁”，系统、全面地了解和掌握PLC控制系统设计方法及最新工程应用技术。

参加本书编写工作的有周志敏、纪爱华、周纪海、纪达奇、刘建秀、顾发娥、刘淑芬、纪和平、纪达安、陈爱华等。本书在写作过程中，无论从资料的收集和技术信息交流上都得到了国内专业学者和同行，以及西门子PLC生产商的大力支持。在此表示衷心的感谢。

由于时间仓促，水平有限，错漏之处在所难免，敬请广大读者批评指正。

编　者

目 录



西门子 PLC 简介

1.1 西门子PLC发展及产品分类

1.1.1 西门子 PLC 发展历程及特点

1. 西门子 PLC 产品发展历程

德国西门子（SIEMENS）公司是欧洲最大的电子和电气设备制造商，SIMATIC 是西门子自动化系列产品品牌统称，诞生于 1958 年，至今已有 50 多年的历史，涵盖了从 PLC、工业软件到 HMI，是全球自动化领导品牌。SIMATIC 的 PLC 系列产品已经成为中国自动化用户最为信赖和熟知的品牌。SIEMENS 公司生产的可编程序控制器在我国的应用相当广泛，在冶金、化工、印刷等领域都有广泛的应用。西门子的 PLC 系列产品发展历程如下。

（1）西门子公司的 PLC 产品 S3 系列是在 1975 年投放市场的，它实际上是带有简单操作接口的二进制控制器。

（2）1979 年微处理器技术被应用到可编程序控制器中，研发出 S5 系列取代了 S3 系列，S5 系列广泛地使用了微处理器技术。

（3）20 世纪 80 年代初，S5 系列进一步升级为 U 系列 PLC，较常用的机型有 S5-90U、S5-95U、S5-100U、S5-115U、S5-135U、S5-155U。

（4）S7 系列诞生于 1994 年 4 月，它具有更国际化、更高性能等级、安装空间更小、更良好的 WINDOWS 用户界面等优势，其机型为 S7-200、S7-300、S7-400、S7-1200。

（5）1996 年，在过程控制领域，西门子公司又提出 PCS7（过程控制系统 7）的概念，将其优势的 WINCC（与 WINDOWS 兼容的操作界面）、Profibus（工业现场总线）、CO-ROS（监控系统）、SINEC（西门子工业网络）及控调技术融为一体。

（6）西门子公司提出 TIA（Totally Integrated Automation）概念，即全集成自动化系统，将 PLC 技术溶于全部自动化领域。

西门子公司的 PLC 产品由最初的 S3 系列发展至今的 S7 系列，目前，S3、S5 系列 PLC 已逐步退出市场，停止生产，而 S7 系列 PLC 发展成为了西门子自动化系统的控制核心，而 TDC 系统沿用 SIMADYND 技术内核，是对 S7 系列产品的进一步升级，它是西门子自动化系统最尖端，功能最强的可编程控制器。

2. 西门子 PLC 的特点

（1）可靠性高，抗干扰能力强。高可靠性是电气控制设备的关键性能，西门子 PLC 由

于采用现代大规模集成电路技术，采用严格的生产工艺制造，内部电路采取了先进的抗干扰技术，具有很高的可靠性。S7 系列 PLC 平均无故障时间高达 30 万 h，一些使用冗余 CPU 的西门子 PLC 的平均无故障工作时间则更长。从西门子 PLC 的机外电路来说，使用西门子 PLC 构成控制系统和同等规模的继电器系统相比，电气接线及开关接点已减少到数百甚至数千分之一，故障也就大大降低。此外，西门子 PLC 带有硬件故障自我检测功能，出现故障时可及时发出警报信息。在应用软件中，应用者还可以编入外围器件的故障自诊断程序，使系统中除西门子 PLC 以外的电路及设备也获得故障自诊断保护。

(2) 配套齐全，功能完善，适用性强。西门子 PLC 发展到今天，已经形成了大、中、小各种规模的系列化产品，可以用于各种规模的工业控制场合。除了逻辑处理功能以外，现代 PLC 大多具有完善的数据运算能力，可用于各种数字控制领域。近年来 PLC 的功能单元大量涌现，使 PLC 渗透到了位置控制、温度控制、CNC 等各种工业控制中。加上西门子 PLC 通信能力的增强及人机界面技术的发展，使用西门子 PLC 组成各种控制系统变得非常容易。

(3) 易学易用，深受工程技术人员欢迎。西门子 PLC 作为通用工业控制计算机，是面向工矿企业的工控设备。它接口容易，编程语言易于为工程技术人员接受。梯形图语言的图形符号与表达方式和继电器电路图相当接近，只用 PLC 的少量开关量逻辑控制指令就可以方便地实现继电器电路的功能。为不熟悉电子电路、不懂计算机原理和汇编语言的人使用计算机从事工业控制打开了方便之门。

(4) 系统的设计、建造工作量小，维护方便，容易改造。西门子 PLC 用存储逻辑代替接线逻辑，大大减少了控制设备外部的接线，使控制系统设计及建造的周期大为缩短，同时维护也变得容易起来。更重要的是使同一设备经过改变程序改变生产过程成为可能，这很适合多品种、小批量的生产场合。

(5) 体积小，质量轻，能耗低。以超小型西门子 PLC 为例，新推出的产品底部尺寸小于 100mm，质量小于 150g，功耗仅数瓦。由于体积小很容易装入机械内部，是实现机电一体化的理想控制设备。

1.1.2 西门子 PLC 产品分类

一般来说可以从三个角度对可编程序控制器进行分类，①按可编程序控制器的控制规模大小分类；②按可编程序控制器的性能高低分类；③按可编程序控制器的结构特点分类。

(1) 按控制规模分类。

1) 小型机。小型机的控制点一般在 256 点之内，适合于单机控制或小型系统的控制。西门子小型机有 S7-200：处理速度 0.8～1.2ms；存储器 2k；数字量 248 点；模拟量 35 路。

2) 中型机。中型机的控制点一般不大于 2048 点，可用于对设备进行直接控制，还可以对多个下一级的可编程序控制器进行监控，它适合中型或大型控制系统的控制。西门子中型机有 S7-300：处理速度 0.8～1.2ms；存储器 2k；数字量 1024 点；模拟量 128 路。

3) 大型机。大型机的控制点一般大于 2048 点，不仅能完成较复杂的算术运算还能进行复杂的矩阵运算。它不仅可用于对设备进行直接控制，还可以对多个下一级的可编程序控制器进行监控。西门子大型机有 S7-400：处理速度 0.3ms/1k 字；存储器 512k；I/O 点

12672。

（2）按控制性能分类。

1）低档机。这类可编程序控制器，具有基本的控制功能和一般的运算能力。工作速度比较低，能带的输入/输出模块的数量比较少。比如，德国 SIEMENS 公司生产的 S7-200 就属于这一类。

2）中档机。这类可编程序控制器，具有较强的控制功能和较强的运算能力。它不仅能完成一般的逻辑运算，也能完成比较复杂的三角函数、指数和 PID 运算。工作速度比较快，能带的输入/输出模块的数量也比较多，输入/输出模块的种类也比较多。比如，德国 SIEMENS 公司生产的 S7-300 就属于这一类。

3）高档机。这类可编程序控制器，具有强大的控制功能和强大的运算能力。它不仅能完成逻辑运算、三角函数运算、指数运算和 PID 运算，还能进行复杂的矩阵运算。工作速度很快，能带的输入/输出模块的数量很多，输入/输出模块的种类也很全面。这类可编程序控制器可以完成规模很大的控制任务。在联网中一般做主站使用。比如，德国 SIEMENS 公司生产的 S7-400 就属于这一类。

（3）按结构分类。

1）整体式。整体式结构的可编程序控制器把电源、CPU、存储器、I/O 系统都集成在一个单元内，该单元叫做作基本单元。一个基本单元就是一台完整的 PLC。控制点数不符合需要时，可再接扩展单元。整体式结构的特点是非常紧凑、体积小、成本低、安装方便。

2）组合式。组合式结构的可编程序控制器是把 PLC 系统的各个组成部分按功能分成若干个模块，如 CPU 模块、输入模块、输出模块、电源模块等。其中各模块功能比较单一，模块的种类却日趋丰富。比如，一些可编程序控制器，除了一些基本的 I/O 模块外，还有一些特殊功能模块，像温度检测模块、位置检测模块、PID 控制模块、通信模块等。组合式结构的 PLC 特点是 CPU、输入/输出均为独立的模块。模块尺寸统一、安装整齐、I/O 点选型自由、安装调试、扩展、维修方便。

3）叠装式。叠装式结构集整体式结构的紧凑、体积小、安装方便和组合式结构的 I/O 点搭配灵活、安装整齐的优点于一身，它也是由各个单元的组合构成。其特点是 CPU 自成独立的基本单元（由 CPU 和一定的 I/O 点组成），其他 I/O 模块为扩展单元。在安装时不用基板，仅用电缆进行单元间的连接，各个单元可以一个个的叠装，使系统达到配置灵活、体积小巧。

1.2 西门子S7系列PLC产品特性

1.2.1 西门子 S7-200/300/400 特性

西门子 S7 系列 PLC 具有体积小、速度快、标准化，具有网络通信能力，功能更强，可靠性更高等特点。S7 系列 PLC 产品可分为微型 PLC（如 S7-200），小规模高性能 PLC（如 S7-300）和中规模高性能的 PLC（如 S7-400）等。

1. 西门子 S7-200 系列 PLC 特性

西门子 S7-200 系列 PLC 是超小型化的 PLC，适用于各行各业，各种场合中的自动检

测、监测及控制。S7-200 系列 PLC 的强大功能使其无论单机运行，或连成网络都能实现复杂的控制功能。S7-200 系列 PLC 可提供 4 个不同的基本型号与 8 种 CPU。

从 CPU 模块的功能来看，西门子 S7-200 系列 PLC 发展至今大致经历了两代：第一代产品其 CPU 模块为 CPU21X，主机都可进行扩展，它具有四种不同结构配置的 CPU 单元：CPU212、CPU214、CPU215 和 CPU216。第二代产品的 CPU 模块为 CPU22X，是在 21 世纪初投放市场的，速度快，具有较强的通信能力。它具有四种不同结构配置的 CPU 单元：CPU221、CPU222、CPU224 和 CPU226，除了 CPU221 之外，其他都可加扩展模块。

针对低性能要求的模块化小控制系统，西门子 S7-200 系列 PLC 最多可有 7 个模块的扩展能力，在模块中集成背板总线的网络连接有 RS-485 通信接口和 Profibus 两种，可通过编程器 PG 访问所有模块，带有电源、CPU 和 I/O 的一体化单元设备。其中扩展模块（EM）有：数字量输入模块（DI）（24VDC 和 120/230VDC）、数字量输出模块（DO）（24VDC 和继电器）、模拟量输入模块（AI）（电压、电流、电阻和热电偶）、模拟量输出模块（AO）（电压和电流）。

还有一个比较特殊的模块是通信处理器（CP），该模块的功能是可以把西门子 S7-200 系列 PLC 作为主站连接到 AS-接口（传感器和执行器接口），通过 AS-接口的从站可以控制多达 248 个设备，这样就可以显著的扩展西门子 S7-200 系列 PLC 的输入/输出点数。

2. 西门子 S7-300 系列 PLC 特性

西门子 S7-300 系列 PLC 为模块化结构，易于实现分布式的配置，因其具有性价比高、电磁兼容性强、抗震动冲击性能好，使其在广泛的工业控制领域中，成为一种既经济又切合实际的解决方案。

西门子 S7-300 系列是模块化小型 PLC，能满足中等性能要求的应用。各种单独的模块之间可进行广泛组合构成不同要求的系统。与 S7-200 系列 PLC 比较，S7-300 系列 PLC 采用模块化结构，具备高速（0.6～0.1μs）的指令运算速度；用浮点数运算比较有效地实现了更为复杂的算术运算；一个带标准用户接口的软件工具方便用户给所有模块进行参数赋值；方便的人机界面服务已经集成在西门子 S7-300 系列 PLC 的操作系统内，人机对话的编程要求大大减少。

SIMATIC 人机界面（HMI）从 S7-300 系列 PLC 中取得数据，S7-300 系列 PLC 按用户指定的刷新速度传送这些数据。S7-300 操作系统自动地处理数据的传送；CPU 智能化的诊断系统连续监控系统的功能是否正常、记录错误和特殊系统事件（例如超时、模块更换等）；多级口令保护可以使用户高度、有效地保护其技术机密，防止未经允许的复制和修改；S7-300 系列 PLC 设有操作方式选择开关，操作方式选择开关像钥匙一样可以拔出，当钥匙拔出时，就不能改变操作方式，这样就可防止非法删除或改写用户程序。S7-300 系列 PLC 可通过编程软件 Step7 的用户界面提供通信组态功能，这使得组态非常容易、简单。S7-300 系列 PLC 具有多种不同的通信接口，并通过多种通信处理器来连接 AS-I 总线接口和工业以太网总线系统；串行通信处理器用来连接点到点的通信系统；多点接口（MPI）集成在 CPU 中，用于同时连接编程器、PC 机、人机界面及其他 SIMATICS7/M7/C7 等自动化控制系统。

相比较 S7-200 系列 PLC，S7-300 系列 PLC 针对的是中型系统，它的模块可以扩展多达 32 个模块，背板总线也在模块内集成，它的网络连接已比较成熟和流行，有 MPI、工业以

太网，使通信和编程变得简单，选择性也比较多，并可借助工具进行组态和参数设置。

S7-300 系列 PLC 的模块稍微多一点，除了信号模块（SM）和 S7-200 的 EM 模块同类型之外，它还有接口模块（IM）用来进行多层组态，把总线从一层传到另一层；占位模块（DM）为没有设置参数的信号模块保留一个插槽或为以后安装的接口模块保留一个插槽；功能模块（FM）执行特殊功能，如计数、定位、闭环控制，相当于对 CPU 功能的一个扩展或补充；通信处理器（CP）提供点对点连接、Profibus 和工业以太网。

新一代的 S7-300 系列 CPU 与以前对应版本备件兼容，具备以下特点：在性能方面提升了 2 倍或者更高。在内存方面：CPU314 从 96KB 扩展到 128KB，CPU315-2DP 从 128KB 扩展到 256KB，CPU315F-2DP 从 192KB 扩展到 384KB。此外，可以同时在线监控两个块，技术数据也趋于一致，I/O 过程映像区增大。同时，CPU315（F）-2DP 的 Profibus 可以使用同步模式，并带有可以进行数据设置的路由。

新一代的 S7-300 系列 PLC 的 CPU 性能比现有的 312、314 和 315（F）-2DPCPU 有了显著提升，例如，新一代 CPU 的用户程序执行速度是原来 CPU 的 2 倍或更高，位运算时间缩减到 50ns，字运算时间缩减到 90ns，定点和浮点数运算性能也有了较大的提升。

新一代 S7-300 系列 PLC 固件版本 V3.0CPU 可以同时在线监控两个块，用户可以选择在一个 PG 或 PC 上同时监视两个块或在两个 PG 或 PC 上同时监控一个块。此外，增加了在块状态中监视的程序行数，只有在 STEP7V5.4SP5 中才有这个功能。

针对 CPU 设计模式选择器有：MRES＝模块复位功能；STOP＝停止模式，程序不执行；RUN＝程序执行，编程器只读操作；RUN-P＝程序执行，编程器可读写操作。状态指示器：SF，BATF＝电池故障；DC5V＝内部 5Vdc 电压指示；FRCE＝表示至少有一个输入或输出被强制；RUN＝当 CPU 启动时闪烁，在运行模式下常亮；STOP＝在停止模式下常亮，有存储器复位请求时慢速闪烁，正在执行复位时快速闪烁。MPI 接口用来连接到编程设备或其他设备，dp 接口用来直接连接到分布式 I/O。

3. 西门子 S7-400 系列 PLC 特性

西门子 S7-400 PLC 是用于中、高档性能范围的可编程序控制器。S7-400PLC 采用模块化无风扇的设计，可靠耐用，同时可以选用多种级别（功能逐步升级）的 CPU，并配有多种通用功能的模板，这使用户能根据需要组合成不同的专用系统。当控制系统规模扩大或升级时，只要适当地增加一些模板，便能使系统升级和充分满足需要。

西门子 S7-400 系列 PLC 具有的模板扩展和配置功能，使其能够按照每个不同的需求灵活组合。一个系统包括：电源模板、中央处理单元（CPU）、各种信号模板（SM）、通信模板（CP）、功能模板（FM）、接口模板（IM）、西门子 S5 模板。

S7-400 系列同 S7-300 系列 PLC 的区别主要在于热启动（wrst）这一部分，其他基本一样。它还有一个外部的电池电源接口，当在线更换电池时可以向 RAM 提供后备电源。编程设备主要有 PG720/PG740/PG760（可以理解成装有编程软件的手提电脑），也可以直接用安装有 Step7（SIEMENS 的编程软件）的 PC 来完成。而实现通信（要编程首先要和 PLC 的 CPU 通信上）的主要接口有：

（1）可以在 PC 上装 CP5611 卡，其上面的 MPI 口可用电缆直接连接。

（2）加个 PC 适配器可把 MPI 口转换成 RS-232 口后接到 PC 上。

（3）PLC 加 CP343 卡后可使它具有以太网口。

4. 西门子 S7-200 与 S7-300/400 的区别

西门子 S7-200 与 S7-300/400 系列 PLC 的主要区别是 PLC 的等级不同和模块差别，S7-200 系列 PLC 属于基础入门级，而 S7-300 和 S7-400 系列 PLC 相对于较高端的应用。即 S7-200 系列 PLC 属于小型机，用于小型的电气控制系统中，着重于逻辑控制；S7-200 也是多功能机，将所有功能结合在一起，它的控制规模最大 512 点，CPU 的运算处理速度不及中大型机快，小型机多为整体式，扩展模块最多可加 8 块，适用于小型设备，性价比高。

S7-300 系列 PLC 属于中型机，用于稍大系统，可实现复杂的工艺控制，如 PID、脉宽调制等；S7-400 系列 PLC 用于中大型控制系统，主要是实现冗余控制。中大型机结构是模块化的，最多可加 300 多块扩展模块，中大型机硬件较贵，成本高，但其运算处理速度快，有很强的通信功能，主要应用于中大型生产线。

（1）硬件区别。S7-200 系列 PLC 是整体式的，CPU 模块、I/O 模块和电源模块都在一个模块内，称为 CPU 模块；而 S7-300/400 系列 PLC 从电源、I/O、CPU 都是单独模块的。但 S7-200 系列 PLC 也可以扩展，只是 CPU 模块集成了部分功能，一些小型系统不需要另外定制模块，S7-200 系列 PLC 的模块也有信号、通信、位控等模块。

S7-200 系列 PLC 对机架没有什么概念，称之为导轨。为了便于分散控制，S7-300/400 系列 PLC 的模块装在一根导轨上的，称之为一个机架，与中央机架对应的是扩展机架，机架还在软件里反映出来。

S7-200 系列 PLC 的同一机架上的模块之间是通过模块正上方的数据接头联系的；而 S7-300/400 系列 PLC 则是通过在底部的 U 型总线连接器连接的。

S7-300/400 系列 PLC 的 I/O 输入是接在前连接器上的，前连接器再接在信号模块上，而不是 I/O 信号直接接在信号模块上，这样可以在更换信号模块而不用重新接线。S7-300/400 系列 PLC 的 CPU 带有 Profibus（Profibus 是一种国际化、开放式、不依赖于设备生产商的现场总线标准）接口。

（2）软件区别。S7-200 系列 PLC 使用的 Step7-Micro/WIN32 软件；S7-300/400 系列 PLC 使用的是 Step7 软件，带有 Micro 和不带的区别是相当的明显的。S7-200 系列 PLC 的编程语言有三种：语句表（STL）、梯形图（LAD）、功能块图（FBD）；S7-300/400 系列 PLC 除了这三种外，还有结构化控制语言（SCL）和图形语言（S7graph），其中 SCL 就是一种高级语言，S7-300/400 系列 PLC 软件最大的特点就是提供了一些数据块来对应每一个功能块（FunctionBlock-FB），称之为 Instance。

1.2.2 西门子 S7-1200/1500 特性

1. 西门子 S7-1200 系列 PLC 特性

西门子 S7-1200 系列 PLC 是低端的离散自动化系统和独立自动化系统中使用的小型控制器模块，S7-1200 系列 PLC 具有集成 PROFINET 接口、强大的集成工艺功能和灵活的可扩展性等特点，充分满足于中小型自动化系统的需求。在研发过程中充分考虑了系统、控制器、人机界面和软件的无缝整合和高效协调的需求。S7-1200 系列 PLC 的问世，标志着西门子在原有产品系列的基础上拓展了产品，代表了未来小型可编程控制器的发展方向。

S7-1200 是紧凑型 PLC，是 S7-200 的升级版，具有模块化、结构紧凑、功能全面等特点，适用于多种应用，能够保障现有投资的长期安全。它采用更快的处理芯片，布尔运算执

行速度从S7-200的0.22μs提升到0.08μs，提升幅度达275%，非常接近S7-300的水平，而且经过测试，S7-1200与S7-300计算速度基本一致，大幅领先S7-200。它采用的CPU工作存储器远超S7-200的存储器，支持存储卡的容量甚至超过了S7-300所支持的存储卡容量，标配PROFINET以太网接口，以及全面的集成工艺功能，可以作为一个组件集成在完整的综合自动化解决方案中。S7-1200的产品新特性如下。

（1）紧凑模块化结构。S7-1200产品延续了S7-200紧凑式结构，CPU1214C的宽度仅有110mm，CPU1212C和CPU1211C的宽度也仅有90mm。通信模块和信号模块的体积也十分小巧，使得这个紧凑的模块化系统大大节省了空间，从而在安装过程中为用户提供了最高的效率和灵活性。另外S7-1200增加一个特殊结构的I/O模块叫作信号板，它是镶嵌在CPU箱体上的分别为2DI/O和1AO，这正是西门子设计精髓之道，可以随时定制所需要补充的I/O模块，中小型工程的问题突显之处就是工程的不确定性，很有可能在工程实施过程当中出现DI/O和AO不够用，而AI却是能够较为富裕信号通道。

（2）强大的控制功能。系统集成了16路PID控制回路，并且PID都是能够支持自适应的快速功能块，并且提供了PID参数调试和观测的控制画面，可以让用户在并不熟悉PID参数如何调整的情况下把工艺参数控制到所需标准。系统集成了多达6个高速计数器（3个100kHz，3个30kHz），用于精确监视增量编码器、频率计数或对过程事件进行高速计数。系统集成了2个高速输出，可用作高速脉冲输出或脉宽调制输出。当组态成PTO时，它们将提供最高频率为100kHz的50%占空比高速脉冲输出，以便对步进电动机或伺服驱动器进行开环速度控制和定位控制。通过2个高速计数器对高速脉冲输出进行内部反馈。当组态成PWM输出时，将生成一个具有可变占空比的固定周期输出来控制电动机速度、阀位置或加热元件的占空比。系统支持对步进电动机和伺服驱动器进行开环速度控制和位置控制。对该功能的组态十分简单：通过一个轴工艺对象和通用的PLC open运行功能块即可实现。除了返回（home）和点动（jog）功能以外，还支持绝对、相对和速度运动。

（3）经典的编程模式。S7-1200使用SIMATIC Step7 Basic工具编程，而这款的工具的使用风格基本与Step7 Professional一样，提供LAD和FBD两种编程语言，并采用OB组织块、FB功能块、FC功能函数、DB数据块的编程形式（通过背景DB的支持可以实现功能块参数化调用）。

（4）复杂的数据结构。复杂的数据结构就是数组、结构等这样的多元素组成的数据单位，而市面上很少会有低端PLC的编程语言能够支持复杂的数据结构，都是采用扁平式的数据类型（BOOL、INT、WORD、DWORD、REAL）。S7-1200这款产品继承了300/400中高端PLC所具备的数据结构，开始支持数组和结构等。

（5）指令参数的多态性。在西门子的编程指令中都是采用数据类型一致分类，例如，加、减、乘、除的指令根据不同的数据类型是不同的指令，而在对S7-1200编程时不分数据类型只是调用功能，让功能块放置在network中时，才会让用户选择是哪种的数据类型，这就轻松实现了参数的多态性。

（6）基于控制对象编程。S7-1200增加了DB数据块和STRUCKT数据类型，正因为具有了这两个必备的条件这才引出此系统的一个很重要的功能，这就是基于控制对象的编辑和编程，添加控制对象也只需要单击一下鼠标。添加新的对象（如一个轴或一个PID控制器）时，工程组态系统的“添加新对象”（Add new object）窗口中会显示相关设置。根据对象

的功能为对象命名。微调各种对象时，用户可以使用功能描述，分配完对象的所有信息后，编辑器中会立即打开该对象。

（7）集成 HMI 工程组态。SIMATIC Step7 Basic 包括功能强大的 HMI 软件 SIMATIC WinCC Basic，用于对 SIMATIC HMI 精简系列面板进行高效的编程和组态。高效的工程组态包括，例如，通过智能拖放功能直接使用 HMI 项目中的控制器过程值。HMI 是整个项目的一部分，HMI 数据可始终保持一致性。HMI 和 PLC 之间的连接可以集中定义，还可以创建多个模板并分配给其他画面。完全集成的 HMI 功能使组态 SIMATIC HMI 精简系列面板变得十分方便且高效。

（8）通信集成 Profinet 接口。在当前自动化推崇工业以太网通信的趋势中，西门子的全线产品已经开始“顶盔贯甲”全部武装上了 Profinet 的接口，而唯独低端产品 S7-200 还是停留在以太网通信 S7 协议的这个层面上，这是因为西门子已经把具有 Profinet 接口的 S7-1200 引领上市了。S7-1200 支持传统的以太网 S7 通信，同样也支持 Profinet 工业以太网总线通信，主要是用于 SIMATIC HMI 精简系列面板（用于可视化）；其他控制器（用于 PLC 间的通信）；第三方设备（用于可选的高级集成）。

（9）灵活的第三方通信。与第三方设备通信一直都是 PLC 自动化厂商的软肋，而 S7-1200 配备了 CM 模块支持 RS232/485 以及自身以太网口通信。针对串行通信 RS232/485 采用使用功能块配置帧通信的方式来完成数据流的通信，S7-1200 支持 SEND _ PTP 和 RCV _ PTP 功能块串行通信的封装，这样就意味着很容易封装出来各种串行通信协议。而针对以太网 S7-1200 提供了 TCP 和 UDP 的两种通信方式，并且提供了标准的 T-Send/T-Receive 功能块完善通信解决方案，例如完全可以利用这两组指令封装出来 modbus-TCP 协议库提供给用户。另外系统提供了丰富的字符处理指令库（LEFT、RIGHT、DELETE、INSERT、REPLACE、VAL _ STRG、STRG _ VAL 和 S _ CONV），这就意味着增强了这款产品对通信中 ASCⅡ字符处理的能力，可以和大量第三方进行自定义字符通信（称重、二次仪表、单片机等）。

2. 西门子 S7-1500 系列 PLC 特性

西门子 S7-1500 PLC 是替代 S7-300/400 的新一代 PLC，其软件平台为 TIA 博途。S7-1500 作为新一代大中型 PLC 比 S7-300/400 的各项指标有很大的提高，专为中高端设备和工厂自动化设计，可供用户使用的充足的资源和超高速的运算处理速度，拥有卓越的系统性能，并集成一系列功能，包括运动控制、工业信息安全，以及可实现便捷安全应用的故障安全功能。其创新的设计使调试和安全操作简单便捷，而集成于 TIA 博途的诊断功能通过简单配置即可实现对设备运行状态的诊断，简化工程组态，并降低项目成本。

新型的 SIMATIC S7-1500 控制器除了包含多种创新技术之外，还设定了新标准，最大程度提高生产效率。无论是小型设备还是对速度和准确性要求较高的复杂设备装置，都一一适用。SIMATIC S7-1500 无缝集成到 TIA 博途中，极大提高了工程组态的效率。在 SIMATIC S7-1500 中包含有诸多新特性，最大限度地确保了工程组态的高效性和可用性。SIMATIC S7-1500 采用模块化结构，各种功能皆具有可扩展性。

在每个 S7-1500 控制器中都包含有以下组件：

（1）一个中央处理器（CPU），用于执行用户程序。

（2）一个或多个电源。

（3）信号模块，用作输入/输出，以及相应的工艺模块和通信模块。

SIMATIC S7-1500 控制器以其众多创新功能，在最高性能和用户友好方面设定了新的生产力标准。它与西门子博途（TIAPortal）无缝集成，创造最佳的工程效益。其卓越的系统性能，确保了最短的响应时间和最高的控制质量。结合 PROFINET 作为标准接口，SIMATIC S7-1500 的性能正在成为新参考，极短的系统响应时间大大提高了效率。Technology Integrated 功能通过运动控制功能和 PROFI drive，实现完美的驱动集成。

SIMATIC S7-1500 具备最佳的可用性。基于其每一个细节的众多创新，SIMATIC S7-1500 可以实现快速而轻松的安装、连接、启动。创新的设计和易于操作在操作过程中也表现得淋漓尽致。其集成的系统诊断功能可以自动生成并完整显示，使得系统状态完全一手掌握。它与 TIA 博途的无缝集成降低了项目成本，因为工程和项目规划比以往任何时候都更容易、更有效。此外，SIMATIC S7-1500 提供了一个全面的、端到端的操作概念，实现完整而一致的数据存储。SIMATIC S7-1500 采用模块化结构，各种功能皆具有可扩展性。

（1）为客户提供充足的资源。

1）CPU1516-3PN 编程用的块总数最多为 6000 个，最大数据块 5MB，FB、FC、OB 最大 512KB。用于程序的工作存储器 5MB，用于数据的工作存储器 1MB。

2）I/O 模块最多 8192 个，过程映像分区最多 32 个，过程映像输入、输出分别为 32KB。每个机架最多 32 个模块。

3）运动控制功能最多支持 20 个速度控制轴、定位轴和外部编码器，有高速计数和测量功能。

4）插槽式装载存储器（SIMATIC 存储卡）最大 2GB，可存储项目数据、归档、配方和有关的文档。

5）S7 定时器、计数器分别有 2048 个，IEC 定时器、计数器的数量不受限制。位存储器（M）16KB。

（2）超高速的运算处理速度。

1）SIMATIC S7-1500 的信号处理速度更为快速，极大缩短系统响应时间，进而提高了生产效率。位操作指令的处理时间典型值为 10ns，换句话说，每 1μs 可处理 10 万条位操作指令。浮点数运算指令的处理时间典型值为 64ns。

2）S7-1500 采用当前最快的背板总线和高效的传输协议，保证了快速信号处理。点到点的反应时间不到 500μs。AI、AO 模块的分辨率均为 16 位，8 点 AI 模块每个模块的转换时间为 125μs。数字量输入模块具有 50μs 的超短输入延时。

3）用于计数、测量和定位输入的工艺模块 TMPos Input 的最高信号频率为 1MHz，4 倍速时为 4MHz。可用 RS-422 接口连接脉冲编码器，支持等式模式、诊断中断和硬件中断。

4）采用 PROFINET IRT 通信可以保证确定的反应时间和高精度的系统响应，最短循环时间为 250μs。

5）通信。SIMATIC S7-1500 带有多达 3 个 PROFINET 接口。其中，两个端口具有相同的 IP 地址，适用于现场级通信；第三个端口具有独立的 IP 地址，可集成到公司网络中。通过 PROFINETIRT，可定义响应时间并确保高度精准的设备性能。

6）集成 WebServer。无须亲临现场，即可通过 Internet 浏览器随时查看 CPU 状态。过程变量以图形化方式进行显示，同时用户还可以自定义网页，这些都极大地简化了信息的采集操作。

（3）技术集成。SIMATIC S7-1500 可将运动控制功能直接集成到 PLC 中，而无须使用其他模块。通过 PLC open 技术，控制器可使用标准组件连接支持 PROFI drive 的各种驱动装置。此外，SIMATIC S7-1500 还支持所有 CPU 变量的 TRACE 功能，在提高了调试效率的同时优化了驱动和控制器的性能。

1）TRACE 功能。TRACE 功能适用于所有 CPU，不仅增强了用户程序和运动控制应用诊断的准确性，同时还极大优化了驱动装置的性能。

2）运动控制功能。通过运动控制功能可连接各种模拟量驱动装置，以及支持 PROFI drive 的各种驱动装置。同时该功能还支持转速轴和定位轴。

3）PID 控制。控制参数可自动优化，实现了各种组件的快速轻松组态，从而提高了控制质量。

（4）信息安全集成。SIMATIC S7-1500 提供一种更为全面的安全保护机制，包括授权级别、模块保护，以及通信的完整性等各个方面。“信息安全集成”机制除了可以确保投资安全，而且还可持续提高系统的可用性。

1）专有技术保护。加密算法可以有效防范未经授权的访问和修改，这样可以避免机械设备被仿造，从而确保了投资安全。

2）防拷贝保护。可通过绑定 SIMATIC 存储卡或 CPU 的序列号，确保程序无法在其他设备中运行。这样程序就无法拷贝，而且只能在指定的存储卡或 CPU 上运行。

3）访问保护。访问保护功能提供一种全面的安全保护功能，可防止未经授权的项目计划更改。采用为各用户组分别设置访问密码，确保具有不同级别的访问权限。此外，使用安全的 CP1543-1 模块，更加强了集成防火墙的访问保护。

4）操作保护。系统对传输到控制器的数据进行保护，防止对其进行未经授权的访问。控制器可以识别发生变更的工程组态数据或者来自陌生设备的工程组态数据。

西门子自动化和驱动产品具有某些工业安全功能，以支持工厂或设备安全操作，这些功能是整个工业安全机制的重要组成部分。

此外，要确保工厂或设备的安全操作，还须采取适当的预防措施（例如，设备单元保护机制），并将自动化和驱动组件纳入整个工厂或设备先进且全面的工业安全保护机制中，可能使用的任何第三方产品须一并考虑。

（5）设计与操作。SIMATIC S7-1500 包含有诸多新特性，最大限度地确保了工程组态的高效性和可用性。

1）内置 CPU 显示屏。可快速访问各种文本信息和详细的诊断信息，在提高设备可用性的同时，也便于全面了解工厂的所有信息。

2）标准前连接器。标准化的前连接器不仅极大简化了电缆的接线操作，同时还节省了更多的接线时间。

3）集成短接片。通过集成短接片的连接，可以更为灵活便捷地建立电位组。

4）集成的 DIN 导轨可快速便捷地安装自动断路器、继电器之类的其他组件。

5）灵活电缆存放方式。凭借两个预先设计的电缆定位槽装置，即使存放粗型电缆，也

可以轻松地关闭模块前盖板。

6）预接线位置。通过带有定位功能的转向布线系统，无论是初次布线还是重新连接，都非常快速便捷。

7）集成的屏蔽夹。对模拟量信号进行适当屏蔽，可确保高质量地识别信号并有效防止外部电磁干扰。同时，使用插入式接线端子，无须借助任何工具既可实现快速安装。

（6）集成系统诊断。SIMATIC S7-1500 集成有诊断功能，无须再进行额外编程。统一的显示机制可将故障信息以文本方式显示在 TIA 博途、HMI、Web server 和 CPU 的显示屏上。

1）一键生成诊断信息。只需简单一击，无须额外编程操作，既可生成系统诊断信息。整个系统中集成有包含软硬件在内的所有诊断信息。

2）统一的显示机制。无论是在本地还是通过 Web 远程访问，文本信息和诊断信息的显示都完全相同，从而确保所有层级上的投资安全。

（7）使用 TIA 博途进行工程组态。SIMATIC S7-1500 无缝集成到 TIA 博途平台中，该平台是一个适用于所有自动化任务的创新型工程组态软件平台。因此，在使用 SIMATIC S7-1500 进行工程组态时就可以应用 TIA 博途中的所有先进功能。

1）TIA 博途 intuitiv。在直观的用户界面中应用最新的软件技术。

2）TIA 博途 efficient。提高质量，降低工程组态工作量。