西门子S7可编程序控制器
——STEP7 编程指南

崔坚　赵欣　任术才　编著

第2版

西门子工业自动化技术丛书

创新工业　知其道　用其妙

SIEMENS

机械工业出版社
CHINA MACHINE PRESS

西门子（中国）有限公司工业业务领域工业自动化与驱动技术集团

西门子工业自动化技术丛书

西门子 S7 可编程序控制器
——STEP7 编程指南
第 2 版

崔　坚　赵　欣　任术才　编著

机械工业出版社

本书介绍了西门子公司的 PLC 系统硬件、CPU 的存储器、数据区、中断和扫描等与用户编程相关的内容。编者结合多年的使用经验就编程语言的使用、项目的创建、调试功能、通信功能及一些典型指令给出了使用示例。

本书的第 2 版中增加了更多 PROFINET 的内容，以示例的方式介绍了 PROFINET IO 设备快速启动功能、设备替换无需存储介质/PG、网络拓扑诊断功能、通过 Web 功能对 CPU 的变量进行监控、浏览 CPU 及模块的诊断信息及整个网络的拓扑结构，以及 PROFINET IRT（等时实时）的 High flexibility。

本书旨在帮助读者由浅入深地学习使用 STEP 7 软件和西门子公司的 PLC，适合做为广大自动化产品工程师快速、深入地掌握西门子公司 PLC 的参考书。

图书在版编目（CIP）数据

西门子 S7 可编程序控制器：STEP7 编程指南/崔坚等编著. —2 版. —北京：机械工业出版社，2009.12
（西门子工业自动化技术丛书）
ISBN 978-7-111-28718-6

Ⅰ. 西… Ⅱ. 崔… Ⅲ. 可编程序控制器 Ⅳ. TM571.6

中国版本图书馆 CIP 数据核字（2009）第 235277 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：林春泉 责任编辑：赵 任 封面设计：鞠 杨
责任校对：陈立辉 责任印制：洪汉军
北京瑞德印刷有限公司印刷（三河市胜利装订厂装订）
2010 年 1 月第 2 版第 1 次印刷
184mm×260mm · 26.75 印张 · 1 插页 · 665 千字
0001-3000 册
标准书号：ISBN 978-7-111-28718-6
ISBN 978-7-89451-415-8（光盘）
定价：66.00 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
社服务中心：（010）88361066
销 售 一 部：（010）68326294
销 售 二 部：（010）88379649
读者服务部：（010）68993821

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

序

工业生产率的提高很大程度上取决于工业生产过程中的自动化装置的水平。作为全球自动化领域技术、标准及市场的领导者，西门子公司一直致力于将自动化和驱动产品及系统不断创新，并体现在从传感器、传动设备、可编程序控制器到网络、人机界面、制造执行系统等自控系统的各个层面，着力为用户提供多种创新、可靠、高效、优质的产品、系统、解决方案和服务，在提高用户的行业竞争力的同时，保证用户的最大程度可持续发展，实现长期的投资保障。

西门子公司自动化与驱动集团在生产自动化、过程自动化、楼宇电气安装和电子装配系统领域为中国用户提供全集成自动化（TIA）和全集成能源管理（TIP）解决方案。作为西门子公司全集成自动化和全集成能源管理的控制核心，西门子公司的S7系列PLC集先进的控制理论、完善的自动化功能与现代通信技术于一体。推出10年来，以其灵活的配置、卓越的性能、形式多样、易于扩展的网络通信方式为广大的工业用户所推崇，在中国及全球各个工业领域广泛地成功应用。

《西门子S7可编程序控制器——STEP7编程指南》一书的出版，正是应了广大初学者的要求，由西门子公司中国的资深工程师遵循项目实现的顺序，结合多年技术支持热线的经验，依照入门指南的方式编写而成。在内容上，涵盖了从硬件安装、接线到软件安装、卸载、授权、指令以及网络配置、编程调试等完成项目要涉及的各个方面。对于中国用户在使用产品时，经常遇到的问题给出了解决方案。

希望本书能成为西门子公司产品手册之外的一本学习使用S7-300/400 PLC的系统教材和实用工具书，帮助广大学习、使用西门子公司PLC的用户快速地理解系统结构，全面掌握SIMATIC PLC的应用技能，在项目中充分发挥该产品的功能和性能，从而帮助工业用户提高工业生产率，实现企业最优化运营。

李永利
自动化与驱动集团客户支持部总经理
西门子（中国）有限公司
2009年9月

前　言

STEP7 是用于 SIMATIC PLC 组态和编程的基本软件包，是西门子公司自动化的入门软件，也是西门子公司自动化各系统的平台软件，可以对 S7-300/400、C7、WinAC 及 ET200 系列智能从站进行编程。STEP7 包含了自动化项目中从项目的启动、实施到测试以及服务的每一阶段所需的全部功能。

STEP7 主要包括以下组件：

- SIMATIC 管理器，用于集中管理所有工具以及自动化项目数据。
- 程序编辑器，用于以 LAD、FBD 和 STL 语言生成用户程序。
- 符号编程器，用于管理全局变量。
- 硬件组态，用于组态和参数化硬件。
- 硬件诊断，用于诊断自动化系统的状态。
- NetPro，用于组态 MPI、PROFIBUS、Ethernet 等网络连接。

除了具有对硬件进行参数化和编程功能外，STEP7 还是 TIA（全集成自动化）的系统平台，不同系统的参数化和编程软件以 STEP7 为平台，集成于其中，使整个控制系统包括 PLC、HMI、驱动等系统具有相同的平台和数据库。

TIA 使整个控制系统具有一致性，体现在以下几个方面：

- 统一的数据管理。
- 统一的编程、组态。
- 统一的通信。
- 诊断功能的一致性。

本书以西门子公司的 PLC 及通信为主，介绍了 PLC 系统硬件以及 CPU 的存储器、数据区、中断和扫描这些与用户编程有关的内容。书中以大量篇幅介绍了编程语言的使用、项目的创建、调试功能、通信功能以及一些指令典型的使用示例，结合编者多年的使用经验以及针对性的应用示例，介绍了复杂的间接寻址的各种使用方法，增强读者阅读程序的能力、扩展编程思路。

随着工业以太网的快速发展，现代控制系统对于系统通信的实时性要求越来越高，为了满足先进控制系统的要求，西门子公司推出实时工业以太网（PROFINET），可以使各层控制都使用同一种网络，实现从上到下的一网到底。因此，我们特别推出了本书的第 2 版。与第 1 版相比，第 2 版中添加了 PROFINET 更多的内容，除了原有的连接分布 IO 设备的 PROFINET IO 通信和 CPU 间通信的 PROFINET CBA 的功能外，还增加了 PROFINET IO 的一些新的功能，以示例的方式介绍了 PROFINET IO 设备快速启动功能、PROFINET IO 设备替换无需存储介质/PG、网络拓扑诊断功能、通过 WEB 功能对 CPU 的变量进行监控、浏览 CPU 及模块的诊断信息及整个网络的拓扑结构，以及 PROFINET IRT（等时实时）的 High flexibility。

本书旨在帮助读者由浅入深地理解和使用 STEP7 软件以及西门子公司的自动化系统，

独立地完成自动化项目的安装、调试任务。希望此书成为广大自动化工程师的良师益友。若有不足之处，敬请指出。

作者

2009 年 9 月

目　录

第 1 章　西门子 S7 系列 PLC 系统概述

1979 年西门子公司推出了 S5 系列 PLC（Programmable Logic Controller，可编程序逻辑控制器），经过不同行业多年的应用，系统的稳定性、可靠性及低故障率得到工控界的认可，进入 20 世纪 90 年代，随着现代通信技术和 IT 技术的迅猛发展，S5 系列 PLC 的配置方法、CPU（Central Processing Unit，中央处理器）的处理能力、网络的通信能力越来越不能满足现代化控制的要求，即不能满足对实时性、快速性、大量的网络通信和数据管理、分布式控制、集成现场设备的快速诊断等要求。为了保持西门子公司在工控业的领先地位，1994 年西门子公司推出了 S7 系列 PLC，与 S5 系列 PLC 相比，除了保持原有的控制功能和系统的稳定性外，在 CPU 运算速度、程序执行效率、故障自诊断、网络通信、面向工艺和运动控制功能上有了质的飞跃，并为后续的系统整合打下了良好的基础。根据控制要求和驱动输入、输出点的能力，S7 控制系统划分为 3 个子系列，即 S7-200 系列、S7-300 系列及 S7-400 系列。此外，各种类型的分布式 I/O 系统也被大量地应用。

1.1　S7 系列 PLC 介绍

1.1.1　S7-200 系列 PLC

S7-200 系列是小型 PLC 系统，其 CPU 如图 1-1 所示，具有串行连接的模块化扩展功能，设计紧凑，CPU 集成输入、输出信号接口功能，输入点集成高速计数器、报警和中断等功能，适合最大输入、输出 100 点左右的控制应用。S7-200 系列 PLC 通过通信模块可以扩展不同的网络接口，如通过 CP243-2 模块扩展 ASI（执行器与传感器接口）网络主站接口；通过 EM277 模块扩展现场总线 PROFIBUS－DP 从站接口；通过 CP243-1 模块扩展以太网接口。此外，S7-200 系列 PLC 还具有远程编程、维护功能。S7-200 系列 PLC 简单的定位功能使控制功能更加完善。S7-200 系列 PLC 使用 STEP7 MICRO WIN 软件进行编程，在本书中不作介绍。

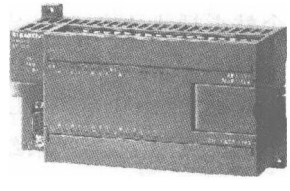


图 1-1　S7-200 系列 PLC CPU

1.1.2　S7-300 系列 PLC

S7-300 系列是中型 PLC 系统，具有模块化扩展功能，设计紧凑，适合最大输入、输出 1000 点左右的控制应用。如图 1-2 所示，S7-300 系列 PLC CPU 中集成了各种中断处理能力，如时间中断、报警中断、循环中断等。S7-300 系列 PLC 具有强大的网络通信能力，如通过 CP343-2 模块可以使 S7-300 系列 PLC 作为 ASI（执行器与传感器接口）网络中的主站，在现场总线 PROFIBUS 的应用中完全支持各种通信方式和服务，在主—从通信方式中，S7-300 系列 PLC 既可以作为 PROFIBUS-DP 的主站，也可以作为从

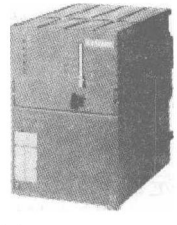


图 1-2　S7-300 系列 PLC CPU

站；在主站间通信方式中，S7-300 系列 PLC 利用不同的通信协议和服务（PROFIBUS-FMS/S7/FDL）可以非常灵活地与通信方进行数据交换；通过工业以太网，S7-300 系列 PLC 之间或与 HMI（Human-Machine Interface，人机接口）可以进行大数据量的通信，利用基于以太网的 PROFINET 总线技术，可以实现数据的实时通信。通过扩展具有独立处理能力的特殊模块，例如功能模块（FM），S7-300 系列 PLC 可以实现高速计数、单轴定位、具有插补功能的 4 轴路径控制，而不会影响 CPU 的处理速度。S7-300 系列 PLC 使用 STEP7 进行编程，是 S7 系列 PLC 的主流产品。

1.1.3 S7-400 系列 PLC

S7-400 系列是大型 PLC 系统，如图 1-3 所示，具有模块化扩展功能，可以连接数万点输入、输出信号。与 S7-300 系列 PLC 相比，S7-400 系列 PLC CPU 中集成了强大的中断处理能力，如数量和种类更多的时间中断、报警中断和循环中断等，即使在同一中断类型中还可以选择不同触发事件的中断；完全覆盖 S7-300 系列 PLC 通信服务和通信协议，在现场总线 PROFIBUS-DP 上实现等时数据通信，保证各个从站的输入信号在 CPU 中同时处理，CPU 的输出命令在各个从站中同时响应；此外，S7-400 系列 PLC 还具有连接更多通信设备的能力和更多的通信资源。同样，S7-400 系列 PLC 通过扩展，具有独立处理能力的功能模块（FM），可以实现高速计数、单轴定位等工艺控制而不会影响 CPU 的处理速度。S7-400 系列 PLC 具有更强的实时处理能力，最多可以在一个站上插入 4 个 CPU 完成同一个控制任务，各 CPU 通过背板总线进行非常快的数据交换。S7-400 系列 PLC 使用 STEP7 进行编程，是 S7 系列 PLC 的主流产品。

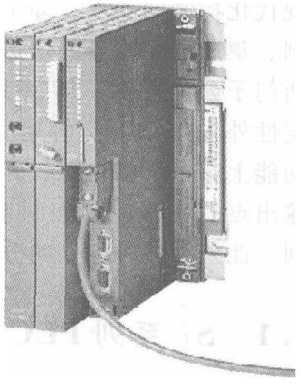


图 1-3 S7-400 系列 PLC CPU

在 S7-400 系列 PLC 中还包括 H（冗余）系统和 F（故障安全）系统，如图 1-4 所示，S7-400H 系统具有冗余的电源、CPU、通信处理器、现场总线、通信接口、输入与输出信号通道等，单一设备故障不会造成整个控制系统的停机，提高了控制系统的可用性；与 S7-400H 冗余系统相比，S7-400F 故障安全系统通过对程序、现场总线、输入与输出信号的再次校验，保证了整个控制系统的可靠性，从而保证了人身的安全以及环境不会遭到破坏。通过一个简单的例子可以区别两个控制系统，例如同一个外部信号分别接入到两个输入模块中，如果其中一路信号连接的模块故障或断线，信号可能在 CPU 中产生差异，对于 S7-400H 系统，将选择预先设定的值继续运行；对于 S7-400F 系统，设备的控制将切换到故障安全模式，通常情况下为停车模式，为了达到设计的安全等级，整个 S7-400F 系统要满足规定的平均无故障时间的要求。

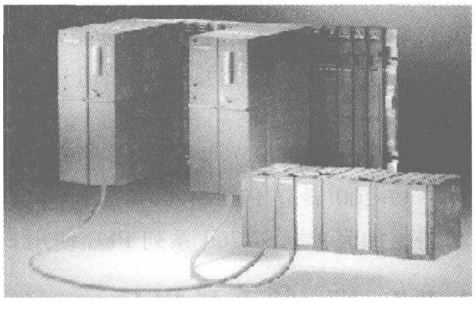


图 1-4 S7-400H CPU

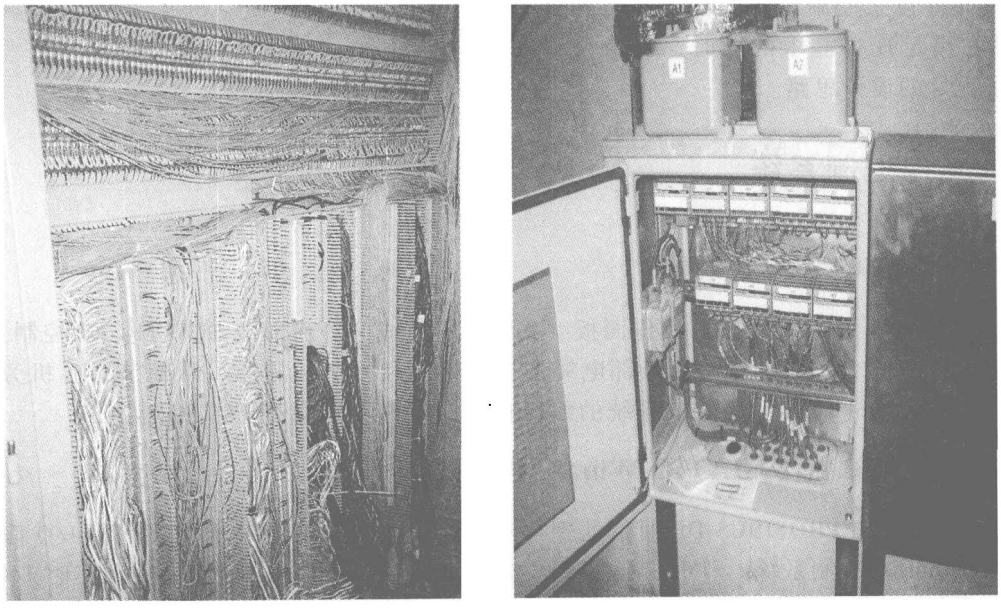
在很多的应用中，将冗余系统和故障安全系统结合使用，如 S7-400H/F，虽然不能提高控制系统的可靠性（F 等级），却可以提高系统的可用性（冗余特点）。STEP7 V5.3 以上版

本已集成冗余系统的配置软件，不需要另外购买，而 F 系统软件需要额外购买。

1.2　远程分布式 I/O

在早期的工厂设计中，选择中央扩展模式安装输入、输出模块，即 CPU 通过背板总线快速地访问 I/O 模块，I/O 模块与 CPU 保持非常近的距离（通常为几米，最远可以扩展到 100m），这样所有外围信号接线汇总到一起，造成 PLC 柜内接线复杂、凌乱，如图 1-5a 所示，对于安装、现场调试以及后期的维护都比较困难。如果现场信号比较远，为了减小信号的衰减而必须选择较粗截面的传输电缆，从而增加了工程的费用。现代工厂设计中，如卷烟厂、物流、钢铁厂，使用大量的远程分布式 I/O 替代原有中央扩展 I/O，这样可以将 I/O 模块放在靠近设备的现场，如图 1-5b 所示，每个远程分布式 I/O 站通过简单的一根现场总线（使用屏蔽双绞线的现场总线 PROFIBUS-DP 或实时工业以太网 PROFINET I/O）与 CPU 进行数据交换。使用远程分布式 I/O 有下列好处：

- 减少布线的时间和工程费用；
- 方便设备的调试；
- 简化后期维护。



a)　　b)

图 1-5　中央扩展 I/O 与远程分布式 I/O 接线对比
a）中央扩展 I/O 接线　b）远程分布式 I/O 接线

不同类型的远程分布式 I/O 站可以满足不同现场的需求，例如在 ET200 远程分布式 I/O 系列中，有适合连接大量 I/O 点的 ET200M；有适合紧凑型的 ET200B；有适合小点数、灵活的 ET200S，如图 1-6 所示。在 ET200S 中，可以安装小功率的负载馈电器，从而节省从站电器柜的安装空间；有适合高防护等级 IP67 的 ET200PRO，如图 1-7 所示；有适合安装于防

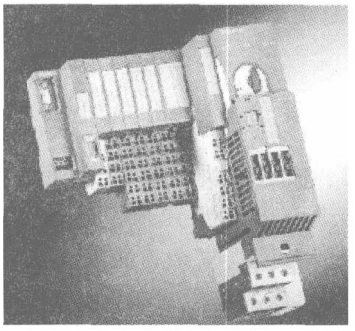


图 1-6 ET200S

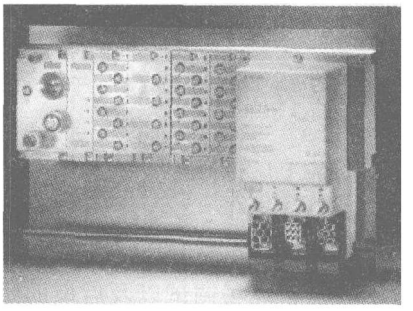


图 1-7 ET200PRO

爆区的 ET200ISP，如图 1-8 所示。除了 ET200 系列外，一些驱动装置、仪表等设备也可以作为分布式 I/O 站与主站 CPU 进行通信。

远程分布式 I/O 站也可以带有 CPU，控制本站的I/O 信号，并与主站进行数据交换，这样的远程站称为智能 I/O 站，在网络或主 CPU 故障时可以独立控制设备。各种类型的分布式 I/O 站在满足现场需求的同时，也给设计人员提供了更好的设计思路。

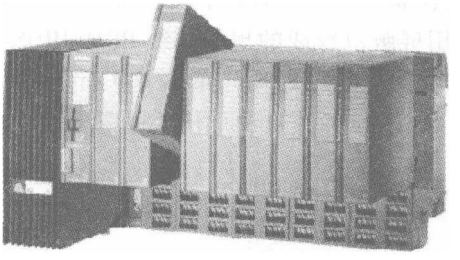


图 1-8 ET200ISP

1.3 其他控制系统

1.3.1 SIMATIC C7 控制器

将 S7-300 系列 PLC 系统与操作面板（OP/TP）集成一体而形成 SIMATIC C7 控制系统，操作面板与 PLC 合二为一不需要外部电缆连接，整体尺寸更加紧凑，从而节省了机旁操作箱的安装空间，SIMATIC C7 控制系统的编程和操作与 S7-300 系列 PLC 相同。

1.3.2 基于 PC 的 SIMATIC WinAC 控制器

在 PC 上安装 PROFIBUS-DP 通信处理器和软件控制器，通过总线连接远程 I/O 而形成 SIMATIC WinAC 控制系统。SIMATIC WinAC 方便集成用户 C/C ++ 程序，插入实时 I/O 卡，可以完成高速响应的控制任务。SIMATIC WinAC 有两种类型：软件 PLC 和插槽型 PLC。

1.4 STEP7 编程软件

1.4.1 编程功能

使用 STEP7 软件可对 S7-300/400 系列 PLC、SIMATIC C7、SIMATIC WinAC 及 ET200 系列智能从站进行编程。STEP7 包含了自动化项目中从启动、实施到测试及维护的每一阶段所

需的全部功能。

STEP7 是用于 SIMATIC PLC 配置和编程的基本软件包。它包括功能强大、适用于各种自动化项目的工具。

STEP7 主要包括以下组件：

- SIMATIC Manager：用于集中管理所有工具以及自动化项目数据。
- 程序编辑器：用于编辑 LAD（梯形图）、FBD（功能块图）和 ST（结构文本）语言生成用户程序。
- 符号编程器：用于编辑符号表和配置通信及消息。
- 硬件配置：用于配置和参数化硬件。
- 硬件诊断：用于诊断自动化系统的状态。

NetPro：

用于配置网络连接及通信。

STEP7 中集成了三种编程语言、通过安装可选软件 Engineer Tool（工程工具），可以扩展编程语言的种类，工程工具面向特定功能，简化和增强自动化控制任务。下列工具可供编程者选择：

（1）S7-SCL

S7-SCL（结构化控制语言）是基于 PASCAL 的高级语言，符合 DIN EN/IEC 61131-3 中定义的高级文本语言 ST（结构文本）。S7-SCL 尤其适用于复杂算法和算术功能的编程以及数据处理任务。

使用 S7-SCL 可以达到下列目的：

- 通过应用功能强大的编程语句（例如 IF... THEN... ELSE），简便、快速、正确地开发程序。
- 改进程序可读性和结构，更易于理解。
- 使用符号生成程序，保证程序的正确修改和重复使用性。
- 使用 Debugger（调试程序），简化在高级语言中的程序调试。

用户可在很短的时间内，经济地为所有自动化任务提供“公式化”的解决方案。

（2）S7-GRAPH

SIMATIC 软件包 S7-GRAPH 基于 STEP7 编程软件。它适合顺控工艺编程，将控制工艺分成不同的“步”，在每一步中填写触发的事件，适合工艺人员使用配置的方式完成工艺编程要求，在标准化的用户界面中可以对实现工艺的“步”进行直观、快速的配置与编程（符合 IEC 61131-3、DIN EN 61131 标准）。

在每个“步”中定义具体的操作（Action）及其执行控制。跳转（Transition）指令控制下一步执行的条件。每一步的执行都根据定义好的互锁和监控条件进行。与 LAD、FBD、STL 相比，其优点如下：

- 直接按工艺流程图生成图形化的程序。
- LAD、FBD 和 STL 主要用于逻辑控制。对于 S7-GRAPH，控制顺序非常重要。
- 采用顺序链，直观图形化地显示控制过程；易于程序维护和调整。
- 在调试阶段可以选择单“步”、手动“步”、自动“步”传送方式进行调试，方便并节省调试时间。

- 采用集成诊断功能进行故障排查，减少停止时间。

（3）S7-HiGRAPH

S7-HiGRAPH 是一种适合于技术工艺人员、编程人员、调试工程师、操作人员以及维护和维修人员的通用工具。

在使用 S7-HiGRAPH 时，示教将代替编程，并通过在状态图中映射技术功能对象（例如阀门、电动机等）来实现。基本宗旨是将自动化任务分为具体的功能单元。技术功能对象或功能单元的特性以状态图的形式加以描述。

工艺人员应首先勾画出大致结构，并定义功能单元及其特性，然后由编程人员处理具体细节。

典型应用：汽车工业（例如发动机、轴和减速箱的制造）、塑料机械、食品和饮料机械、包装机械、机床、卷取机和专用机械。

S7-HiGRAPH 的优点：

- 配置、上线调试以及维护、保养和维修，所有人员均使用相同的工具。
- 点击按钮，即可以根据状态图生成执行程序。
- 通过易于集成的信号传送和监控功能，可以非常简便地检测故障，降低停机的时间。
- 一旦生成状态图，即可反复地使用。

在编辑状态图时，可以将自动化任务拆分为具体的机械功能单元，每个功能单元的特性都以状态图的形式加以描述。各种操作都以状态（State）的形式触发，例如初始化（Initialize）、拧紧（Tighten）、松开（Loosen）。

由于 S7-HiGRAPH 和 S7-GRAPH 工程工具可提供两种不同的生产过程视图，并能相互最佳实现，也可在一个项目当中组合使用。

（4）CFC

CFC（连续功能图）工程工具是专为那些需要为工厂进行配置和编程的工程师而备的。

使用 CFC，可在参数输入的同时，将工艺技术参数转换为可执行的自动化系统程序。它只需将预置模块链接在一起，然后设置其参数即可，无需高级编程知识。

与 LAD、FBD 和 STL 相比，其优点如下：

- 在工程制图阶段即可优化使用。
- 降低图形链接配置要求。
- 重复使用性。
- 上手快速、简单。
- 快速、直观链接预置功能。
- 使用 S7-SCL，简便生成定制模块。
- 生成整个技术工艺程序。
- 控制结构一目了然。
- 离线测试，缩短调试时间。
- 在线修改，高度透明，工厂可用性高。

CFC 工程工具还可用于生成 SIMATIC S7 和 SIMATIC WinAC 自动化解决方案。任何模块都可以根据工艺规范相互链接，例如开环和闭环控制数据，甚至是配置和归档整个信息流。

配置界面是一种绘图界面，设置有预置模块，并根据工艺条件相互链接。对于工程师来