



机电工程类专业“互联网+”创新型精品教材

S7-1200 PLC编程与应用

主编 刘佳

S7-1200 PLC编程与应用

主编 刘佳

北京出版集团
北京出版社



北京出版集团
北京出版社

图书在版编目 (CIP) 数据

S7-1200 PLC 编程与应用 / 刘佳主编. -- 北京: 北京出版社, 2025. 7. -- ISBN 978-7-200-19573-6
I. TM571.61

中国国家版本馆 CIP 数据核字第 2025Q0U539 号

S7-1200 PLC 编程与应用

S7-1200 PLC BIANCHENG YU YINGYONG

主 编: 刘佳
出 版: 北京出版集团
北 京 出 版 社
地 址: 北京北三环中路 6 号
邮 编: 100120
网 址: www.bph.com.cn
总 发 行: 北京出版集团
经 销: 新华书店
印 刷: 定州启航印刷有限公司
版 印 次: 2025 年 7 月第 1 版 2025 年 7 月第 1 次印刷
成品尺寸: 185 毫米 × 260 毫米
印 张: 13.5
字 数: 304 千字
书 号: ISBN 978-7-200-19573-6
定 价: 42.00 元

教材意见建议接收方式: 010-58572341 邮箱: jiaocai@bphg.com.cn

如有印装质量问题, 由本社负责调换

质量监督电话: 010-82685218 010-58572341 010-58572393



目录

项目一 PLC 与 TIA 博途软件

1

- 任务一 初识 PLC 的发展史 1
- 任务二 S7-1200 PLC 的结构 5
- 任务三 S7-1200 PLC 的工作原理 11
- 任务四 S7-1200 PLC 的编程软件 15
- 任务五 S7-1200 PLC 的编程语言 17
- 任务六 S7-1200 PLC 项目的创建与仿真 20

项目二 位逻辑指令

39

- 任务一 多开关控制单台电动机的 PLC 控制 41
- 任务二 多路抢答器 49
- 任务三 单开关控制多台电动机的 PLC 控制 57
- 任务四 单通道双向通行的 PLC 控制 65
- 任务五 搭建 TIA 博途工程项目模板 72

项目三 定时器与计数器指令

78

- 任务一 使用定时器的霓虹灯的自动控制 78
- 任务二 多级生产线的输送系统 93
- 任务三 手自一体交通信号灯控制系统 101
- 任务四 使用计数器的霓虹灯的自动控制 106
- 任务五 手自一体霓虹灯控制系统 120
- 任务六 生产线产量计数显示系统 132
- 任务七 停车场车辆出入库的高级控制——停车场计数
显示系统 143

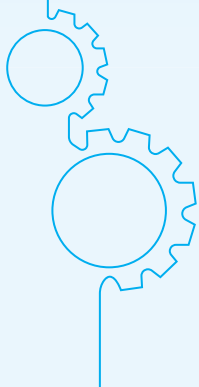
项目四 数据处理与运算指令 148

任务一	炫酷跑马灯的组态控制	148
任务二	自动往返生产线的组态控制	155
任务三	液位的采集与显示的组态控制	162
任务四	多级生产线的组态控制	168
任务五	自动车库门的组态控制	174

项目五 PLC 控制程序设计方法 181

任务一	基于经验设计法的全自动洗衣机	181
任务二	基于 FC 函数的全自动洗衣机	189
任务三	基于 FB 函数块的全自动洗衣机	199

参考文献 208



项目一 PLC 与 TIA 博途软件

人类通过大脑和神经系统对复杂任务进行决策与协调。人的大脑负责逻辑运算、指令下达，神经系统则将信号传递至各个执行器官，完成动作响应。而在工业场景的现代工业自动化与智能控制系统中，机器设备同样需要这样的“大脑”和“神经系统”来实现精准控制。西门子 S7-1200 PLC（可编程逻辑控制器）正是工业自动化领域的核心控制单元，它如同机器的智能中枢，协调传感器、执行器等部件，完成从数据采集到逻辑运算再到动作控制的全流程。本项目主要介绍 PLC 的由来，西门子 S7-1200 系列 PLC，以及相关编程软件——博途软件的应用。

任务一

初识 PLC 的发展史

任务描述

本任务旨在系统梳理可编程逻辑控制器（PLC）的技术发展历程——从 20 世纪 60 年代继电器控制的替代需求到现代智能化工业控制核心的演变，分析其技术突破、功能扩展及对工业自动化的深远影响。通过研究 PLC 的起源、关键发展阶段、核心技术革新以及未来趋势，可以理解 PLC 在工业控制领域不可替代的地位，探讨其与信息技术、物联网等新兴技术的融合方向。



任务目标

1. 理解 20 世纪 60 年代工业控制继电器系统的局限性，分析美国通用汽车公司 (General Motors, GM) 提出“GM 十条”对 PLC 诞生的推动作用，明确第一代 PLC (如 DEC PDP-14) 的设计目标与应用场景。
2. 研究 PLC 从硬接线逻辑到可编程控制、从单一逻辑控制到多功能集成 (如运动控制、通信联网) 的关键技术突破，总结各阶段代表性产品 (如西门子 S5 系列、S7 系列) 的技术特点。
3. 探讨 PLC 在工业 4.0、智能制造中的角色，研究其与物联网的融合方向，理解开放化、模块化、智能化的发展趋势。
4. 通过技术史的学习，树立科学精神与历史责任感，理解工程师在技术革新中的社会责任，强调创新驱动与可持续发展理念在工业自动化领域的实践意义。

任务实施

一、PLC 的定义

可编程逻辑控制器，即可编程控制器，英文全称 programmable logical controller，简称 PLC 或 PC。由于“PC”容易和个人计算机 (Personal Computer) 的英文缩写 PC 混淆，所以人们习惯用“PLC”作为可编程控制器的英文缩写。PLC 是一个以微处理器为核心的数字运算操作电子系统，专为工业现场应用而设计，采用可编程的存储器，用以在其内部存储执行逻辑运算、顺序控制、定时、计数和算术运算等操作指令，并通过输入/输出接口 (又称 I/O 接口)，控制各种类型的机械或生产过程。

二、PLC 的产生

传统的继电接触器 (简称继电器) 控制系统具有结构简单、价格低廉、操作容易、技术难度较小等优点，被长期广泛地应用在工业控制的各个领域。然而，这种系统的如下缺点在现代化生产中日益突出。

- (1) 继电器接点间、接点与线圈间存在大量连接导线，其控制功能单一，更改困难。
- (2) 大量的继电器元器件需集中安装在控制柜内，设备体积庞大，不易搬运。
- (3) 若继电器接点接触不良、导线连接不牢，则往往会导致设备故障频发，且查找、排除故障困难，系统的可靠性较低。
- (4) 继电器动作时固有的电磁动作时间，限制了系统的响应速度。

因此，继电器控制系统越来越难以满足现代化生产控制的要求。特别是产品更新换代、生产线调整时，需要对原有继电器控制系统进行改造，由此产生的经济损失相当可观。

20 世纪 60 年代末期，美国汽车制造业竞争十分激烈。为适应市场要求，完成从少

品种大批量生产向多品种小批量生产的转变，尽可能减少转变过程中控制系统的设计制造时间，降低经济成本，1968 年美国通用汽车公司公开招标，要求用新的控制装置取代生产线上的继电器接触器控制系统，也就是著名的“通用十条”（也称作“GM 十条”），其具体要求如下。

- (1) 编程简单，可在现场修改和调试程序。
- (2) 维护方便，采用插入式模块结构。
- (3) 可靠性高于继电器控制系统。
- (4) 体积小于继电器控制装置。
- (5) 数据可直接送入管理计算机。
- (6) 成本可与继电器控制系统竞争。
- (7) 可直接用 115 V 交流电压输入。
- (8) 输出量为 115 V、2 A 以上，能直接驱动电磁阀、接触器等。
- (9) 通用性强，易于扩展。
- (10) 用户程序存储器容量至少 4 KB。

根据这些要求，美国数字设备公司（DEC 公司）于 1969 年研制出了世界上第一台可编程序控制器 PDP-14，并在 GM 公司的汽车生产线上首次应用成功。当时人们把它称为可编程序逻辑控制器（Programmable Logic Controller），简称 PLC，可编程序控制器由此诞生。由于它主要用来取代继电器逻辑控制，系统功能仅限于执行继电器逻辑、计时、计数等。

PLC 诞生不久即显示了其在工业控制中的重要地位，日本、德国、法国等国家也相继研制成各自的 PLC。PLC 自问世以来，经过近 40 年的发展，在美、德、日、法等工业发达国家已成为重要的产业之一。PLC 的世界总销售额不断上升、生产厂家不断涌现、品种不断翻新，产量产值大幅度上升而价格则不断下降。

目前，世界上有 200 多个厂家生产 PLC，著名的有：美国 AB 电气公司、德州仪器公司；日本三菱、富士、欧姆龙、松下电工等公司；德国西门子公司；法国 TE 施耐德公司；韩国三星、LG 公司等。

三、PLC 的发展概况

PLC 自问世以来，经过几十年的发展，在美、德、日等发达国家已成为重要的产业。其销售额不断上升，生产厂家不断涌现，品种不断翻新，而在产量、产值大幅度上升的同时，价格则不断下降。

四、当前 PLC 的发展方向

(1) 产品规模向大、小两个方向发展。大型 PLC I/O 点数达 14336 点，配有 32 位微处理器和大容量存储器，支持多 CPU 并行工作，扫描速度极高。小型 PLC 整体结构向小型模块化发展，增加了配置的灵活性，降低了成本。

(2) PLC 在闭环控制过程中的应用日益广泛。



(3) 加强通信功能。

(4) 不断推出新的器件和模块。高档的 PLC 除了主要采用高性能 CPU 以提高处理速度外, 还配有带处理器的 EPROM 或 RAM 的智能 I/O 接口模块高速计数模块、远程 I/O 接口模块等专用化模块。

(5) 编程工具丰富多样, 性能不断提高, 编程语言趋于标准化。PLC 的编程工具有各种简单或复杂的编程器及编程软件, 采用梯形图、功能图、语句表等编程语言, 也有高档的 PLC 指令系统。

(6) 发展容错技术。采用热备用或并行工作的工作方式。

(7) 追求软硬件的标准化。

目前, PLC 在国内各行业有着极大的应用, 技术含量也越来越高。

五、PLC 的发展趋势

(一) 高速度、大容量

为了提高 PLC 的处理能力, 就必须要求 PLC 具有更快的响应速度和更大的存储容量。目前, 有的 PLC 的扫描速度可达每毫秒一万步左右。PLC 的扫描速度已成为一个很重要的性能指标。

在存储容量方面, 部分 PLC 的存储空间最高可达数十兆字节。为扩展存储容量, 部分制造商已开始采用磁泡存储器或硬盘。



PLC 新动向

(二) 超大型或超小型

当前中小型 PLC 发展已逐渐成熟, 为了适应市场的不同需要, 今后 PLC 要向多品种方向发展, 特别是向超大型和超小型两个方向发展。现已有 I/O 点数达 14336 点的超大型 PLC, 它使用 32 位处理器和大容量存储器, 支持多 CPU 并行工作, 功能较强。小型 PLC 由整体结构向小型模块化结构发展。这样可以使配置更加灵活。为了满足市场需要, 现在部分生产厂家已开发出各种简易、经济的超小型及微型 PLC, 其最小配置的 I/O 点数为 8~16 点, 以适应单机及小型系统自动控制的需要, 如三菱公司的 FX1N 系列 PLC。

(三) 大力开发智能模块, 增强联网通信能力

为满足各种自动化控制系统的要求, 各生产厂家近年来不断开发出各种功能模块, 如高速计数模块、温度控制模块、远程 I/O 模块、通信和人机接口模块等。这些带 CPU 和存储器的智能 I/O 模块既扩展了 PLC 的功能, 又扩大了 PLC 的应用范围。PLC 的联网通信分为两类: 一类是 PLC 之间的联网通信, 各 PLC 生产厂家都有自己的专有联网手段; 另一类是 PLC 与计算机之间的联网通信, 一般 PLC 都有专用通信模块与计算机通信。为了加强联网通信能力, PLC 生产厂家之间也在协商制订通用的通信标准, 以便构成更大的 PLC 网络系统。

（四）增强外部故障的检测与处理能力

相关统计资料显示，在 PLC 控制系统的故障中 CPU 故障占 5%，I/O 接口故障占 15%，输入设备故障占 45%，输出设备故障占 30%，线路故障占 5%。前两项共计 20% 的故障属于 PLC 的内部故障，它可通过 PLC 本身的软、硬件实现检测、处理；而其余共计 80% 的故障属于 PLC 的外部故障。因此，PLC 生产厂家都在致力于研究、开发用于检测外部故障的专用智能模块，进一步提高系统的可靠性。

（五）编程语言多样化

在 PLC 系统结构不断发展的同时，PLC 的编程语言也越来越丰富，功能也在不断增加。除了大多数 PLC 使用的梯形图语言外，为了适应各种控制要求，出现了面向顺序控制的步进编程语言、面向过程控制的流程图语言、与计算机兼容的高级语言（如 BASIC、C 语言）等。多种编程语言的并存、互补与发展是 PLC 进步的一种表现。

任务二

S7-1200 PLC 的结构

任务描述

本任务旨在系统解析西门子 S7-1200 可编程逻辑控制器 (PLC) 的硬件与软件结构，理解其模块化设计、功能集成与扩展能力。通过研究 S7-1200 的硬件组成（如 CPU 模块、信号模块、通信模块）和软件架构（如 TIA 博途编程环境、程序块结构），掌握其在工业控制中的应用逻辑与配置方法，为实际工程中的设备选型、系统组态和程序开发提供技术支撑。

任务目标

1. 掌握西门子 S7-1200 PLC 的硬件组成与功能模块，包括 CPU 模块、信号模块 (SM)、信号板 (SB)、通信模块 (CM/CP) 的物理结构、接口定义及扩展能力，理解其模块化设计理念与工业环境适配性。
2. 理解 S7-1200 的软件架构，熟悉 TIA 博途 (Portal) 编程环境的核心功能（如程序块组织、数据存储机制、通信协议配置），能通过梯形图 (LAD)、功能块图 (FBD) 等语言实现基本控制逻辑的编写与调试。



任务目标

3. 能够结合实际工程需求，完成 S7-1200 PLC 的硬件选型、系统组态及 I/O 地址分配，并实现与 HMI、变频器等设备的协同控制，验证系统的稳定性和可扩展性。
4. 在学习和实践中强化规范操作意识与技术创新思维，理解工业自动化设备标准化设计的重要性，树立工程师在技术应用中的社会责任感与可持续发展理念。

任务实施

一、S7-1200 PLC 的硬件组成

S7-1200 PLC 的硬件采用模块化设计，可根据实际需求灵活扩展，如图 1-2-1 所示，主要包括以下核心组件。

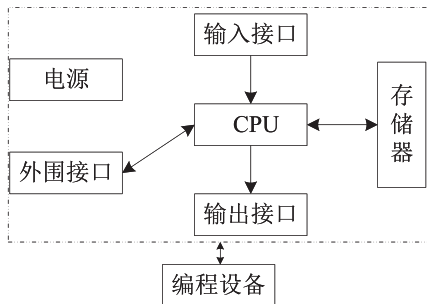


图 1-2-1 S7-1200 PLC 硬件组成

(一) CPU 模块

S7-1200 PLC 硬件如图 1-2-2 所示。S7-1200 PLC 的 CPU 模块作为控制系统的核心，集成了微处理器、电源、I/O 接口、通信接口及运动控制功能。

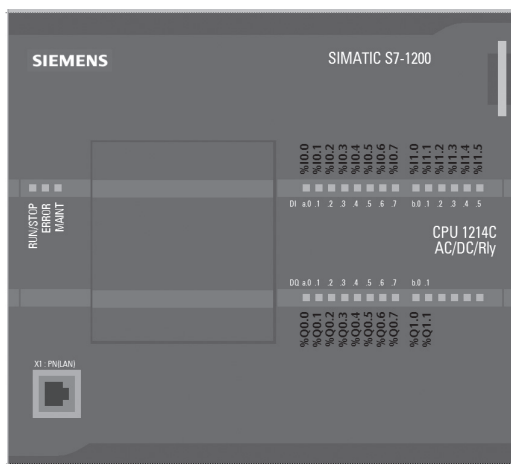


图 1-2-2 S7-1200 PLC 主机 CPU

功能特性：内置数字量 I/O（如 CPU 1214C 支持 14 输入 /10 输出）及模拟量输入（如 2 路 0~10 V 电压输入）；集成 PROFINET 以太网接口，支持编程、HMI 通信及第三方设备交互；支持高速脉冲输出（最高 1 MHz，CPU 1217C）及硬件中断响应。型号差异：不同型号（如 1211C、1214C、1217C）在存储器容量（75~250 KB）、扩展能力（最多 8 个信号模块）及 I/O 点数上有所区别。具体区别如表 1-2-1 所示。

表 1-2-1 S7-1200 PLC 系列不同型号的区别

CPU 型号	CPU1211C	CPU1212C	CPU1214C	CPU1215C	CPU1217C
数字量 I/O 点数	6 入 /4 出	8 入 /6 出	14 入 /10 出	14 入 /10 出	14 入 /10 出
模拟量 I/O 点数	2 入	2 入	2 入	2 入 /2 出	2 入 /2 出
工作 / 装载存储器	50 KB/1 MB	75 KB/2 MB	100 KB/4 MB	125 KB/4 MB	150 KB/4 MB
信号扩展模块	无	2	8	8	8
最大本地数字量 I/O 点数	14	82	284	284	284
最大本地模拟量 I/O 点数	13	19	67	69	69
高速计数器	3	5	6	6	6
脉冲输出	100 kHz	100 k/30 kHz	100 k/30 kHz	100 k/30 kHz	1 M/100 kHz
上升沿 / 下降沿中断点数	6/6	8/8	12/12	12/12	12/12
脉冲捕捉输入点数	6	8	14	14	14
PROFINET 以太网接口	1	1	1	1	2

（二）信号模块

用于扩展数字量 / 模拟量输入输出，实现与现场设备的信号交互。

数字量模块：包括 DI（如 SM 1221）、DO（如 SM 1223）及混合模块，支持开关、传感器等设备的连接，如图 1-2-3 所示。信号模块安装在 S7-1200 PLC 主机的右侧。

信号模块是系统的眼、耳、手、脚，是联系外部现场设备和 CPU 的桥梁。输入模块用来接收和采集输入信号，其中：数字量输入模块用来接收从按钮、选择开关、数字拨码开关、限位开关、接近开关、光电开关、压力继电器等传来的数字量输入信号；模拟量输入模块用来接收电位器、测速发电机和各种变送器提供的连续变化的模拟量电流、电压信号，或者直接接收热电阻、热电偶提供的温度信号。

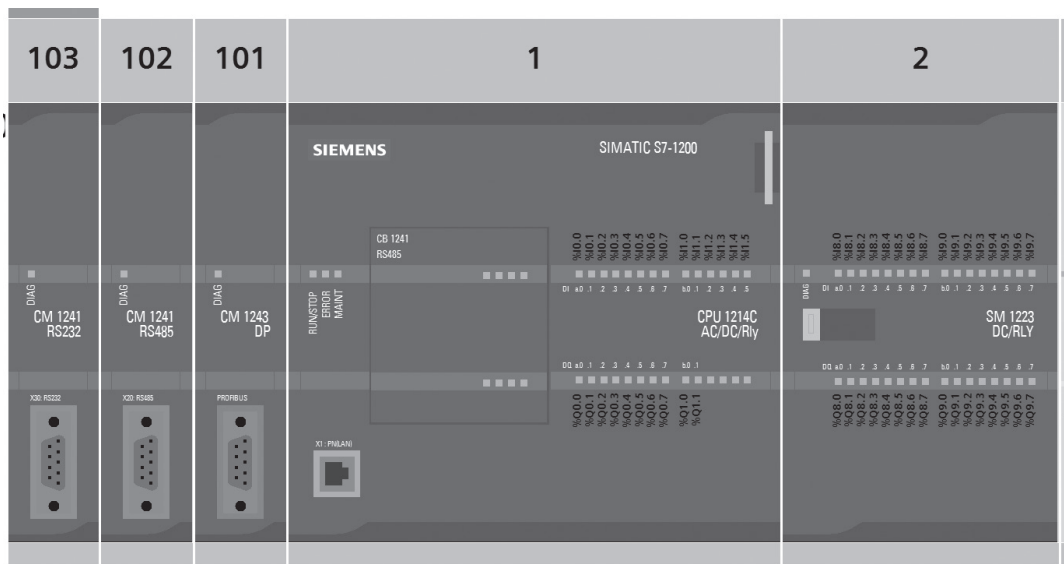


图 1-2-3 S7-1200 PLC 扩展

模拟量输入 (AI): 支持电流 / 电压 (如 $-10\sim 10\text{ V}$)、热电阻 (PT100)、热电偶 (K 型) 等信号;

模拟量输出 (AO): 提供 $-10\sim 10\text{ V}$ 或 $4\sim 20\text{ mA}$ 输出, 用于控制变频器、调节阀。

隔离设计: CPU 模块内部的工作电压一般是 $\text{DC}5\text{ V}$, 而 PLC 的外部输入 / 输出信号电压一般较高, 如 $\text{DC}24\text{ V}$ 或 $\text{AC}220\text{ V}$ 。从外部引入的尖峰电压和干扰噪声可能损坏 CPU 模块中的元器件, 或使 PLC 不能正常工作。在信号模块中, 用光电耦合器、光电晶闸管、小型继电器等器件来隔离 PLC 的内部电路和外部的输入 / 输出电路。信号模块除了传递信号外, 还有电平转换与隔离的作用。

(三) 通信模块

S7-1200 PLC 可以通过添加通信模块来扩展它的联网和交互能力, 让设备更方便地与其他工业设备“对话”。如图 1-2-3 左侧所示。

例如, 它可以加装支持 PROFIBUS (一种工业总线协议)、RS485 (一种标准通信接口) 或 IO-Link (智能传感器专用协议) 的模块, 这些模块直接插在 PLC 主机的左侧, 最多可以装 3 个。有了这些模块, PLC 就能和电脑、其他工业设备甚至不同品牌的第三方设备交换数据 (比如接收传感器信号或控制电机), 还能实现远程软件更新、在线维护和故障诊断, 这就像给设备装上了“联网升级”和“远程维修”的功能包。

(四) 信号板

S7-1200 PLC 的顶部有一个“即插即用”的扩展槽, 可以直接插入小巧的信号板, 像给手机装内存卡一样简单, 无需改变设备原本的尺寸。如图 1-2-3 中间方形位置所示, 例如:

数字量信号板（如 SB 1222）可以扩展开关信号的输入 / 输出（比如控制几个灯或按钮）；

模拟量信号板（如 SB 1231 RTD）能接入温度探头或压力传感器的信号；

通信信号板（如 SB 1232 RS485）则能让 PLC 通过串口连接其他设备。

这种设计特别适合小规模扩展需求的场景，比如工厂里想给设备临时加装一个测温探头（热电偶），或者多控制几台小电机，用这种“迷你扩展卡”既省空间又方便，避免了安装大模块的麻烦。

（五）电源模块与附件

电源模块：提供 24 V-DC 或 120/230 V-AC 电源，如 PS 1207/1208，确保系统稳定供电；

存储卡：SIMATIC 存储卡用于扩展程序存储空间或固件更新；

安装配件：支持 35mm DIN 导轨安装，适配控制柜布局。

以上设计使 S7-1200 兼具紧凑性与功能性，适用于从简单机械控制到复杂过程自动化场景。

二、S7-1200 PLC 的硬件接线

本教材使用西门子 S7-1200 PLC，CPU 型号为 1214C AC/DC/RLY，具体含义如图 1-2-4 所示。

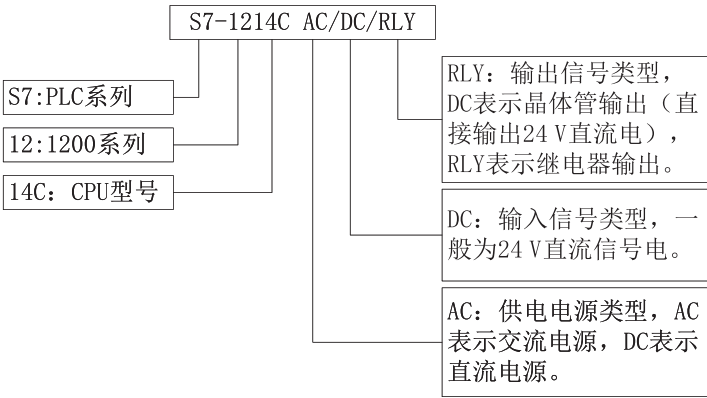


图 1-2-4 S7-1200 PLC 型号含义

（一）电源模块

如图 1-2-5 所示，120~240 V-AC，箭头朝下，表示电源输入；24 V-DC，箭头朝上，表示电源输出。

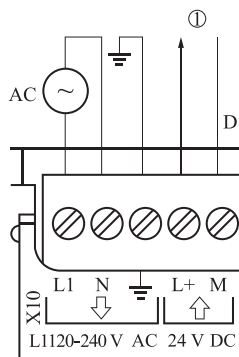


图 1-2-5 电源模块接线图

(二) 信号输入模块

如图 1-2-6 所示，24 V-DC-INPUTS (DI) 表示数字量输入，1214C 内置 14 个数字量输入点。ANALOG INPUTS (AI) 表示模拟量输入，1214C 内置 2 个模拟量输入点。

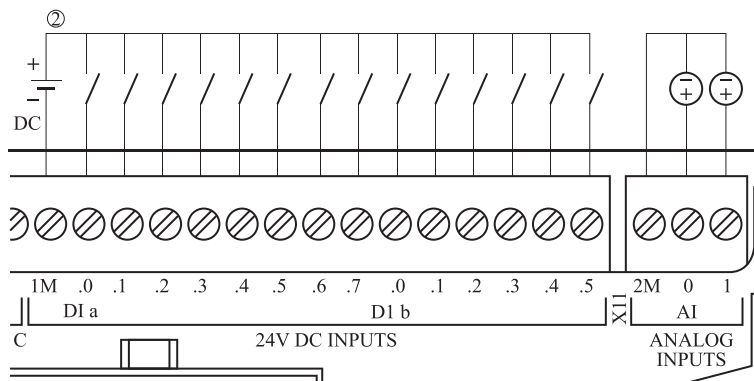


图 1-2-6 信号输入模块接线图

(三) 信号输出模块

如图 1-2-7 所示，RELAY OUTPUTS (RLY) 表示继电器输出，1214C 内置 10 个数字量输出点。

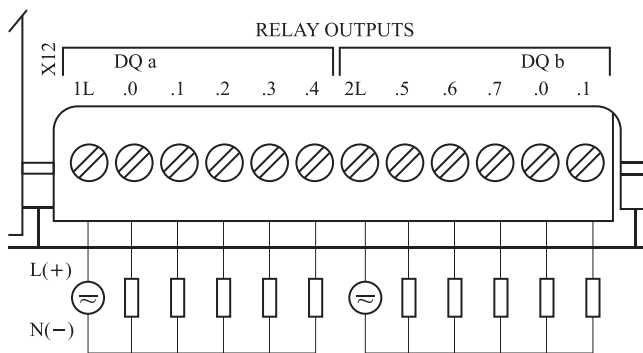


图 1-2-7 信号输出模块接线图

任务三

S7-1200 PLC 的工作原理

任务描述

本任务旨在深入解析西门子 S7-1200 可编程逻辑控制器 (PLC) 的核心工作原理，涵盖其硬件信号处理机制、软件程序执行流程及系统协同控制逻辑。通过研究 S7-1200 的输入 / 输出 (I/O) 信号采集与响应、中央处理单元 (CPU) 的扫描周期 (输入采样、程序执行、输出刷新)，理解和掌握其在工业控制中的实时性、可靠性和扩展性设计。结合 TIA 博途 (Portal) 编程环境，实践 PLC 程序的编写、仿真调试及与外部设备 (如 HMI、传感器、执行器) 的协同控制，为工业自动化系统的设计与优化提供理论基础与技术支持。

任务目标

1. 理解 S7-1200 PLC 的硬件工作原理，包括输入模块 (如数字量 / 模拟量信号采集)、输出模块 (如继电器 / 晶体管驱动执行器) 与中央处理器 (CPU) 的协同工作流程，掌握信号从输入到逻辑处理再到输出的完整链路机制。
2. 掌握 S7-1200 的程序执行机制，包括扫描周期 (输入采样→程序执行→输出刷新) 的时序控制、中断事件 (如硬件中断、通信中断) 的优先级响应，以及多任务程序块 (OB、FB、FC) 的调用逻辑，能够分析程序执行效率与资源占用的优化方法。
3. 通过 TIA 博途软件编写并仿真调试 PLC 程序，结合具体工业场景 (如电机启停控制、PID 温度调节) 验证逻辑控制功能，理解 PLC 在复杂系统中的实时性与可靠性设计原则。
4. 在学习和实践中强化工业安全规范意识，理解 PLC 系统抗干扰设计、故障诊断机制的重要性，培养严谨的工程思维与技术创新能力，树立技术服务于安全生产和社会可持续发展的责任感。



任务实施

一、S7-1200 PLC 的工作过程

(一) 工作模式：PLC 的三种核心状态

西门子 S7-1200 PLC 作为工业控制的核心设备，其工作模式类似于电脑的操作系统状态。S7-1200 PLC 有以下三种工作模式。

1. STOP 模式（停机模式）

这是 PLC 的“待机休眠”状态。在此模式下，CPU（中央处理器）会完全停止执行用户编写的控制程序，但允许工程师通过 TIA 博途软件（类似 PLC 的“操作系统”）对设备进行配置和调试，例如上传或下载新的控制程序、修改硬件模块的参数设置（如调整输入信号的滤波时间），或者在线查看设备状态。此时所有输出模块会自动切断电源，确保连接的电机、阀门等设备处于安全状态，防止误动作。

2. STARTUP 模式（启动模式）

当 PLC 通电开机或从 STOP 模式切换到 RUN 模式时，会进入这个“启动准备”阶段，类似于电脑的开机自检过程。此时 PLC 会执行一系列初始化操作，包括清除临时数据（如复位没有设置“保持功能”的定时器、计数器）、配置通信接口、检查扩展模块的连接状态，并执行用户预设的启动程序（OB100 组织块）。例如让设备启动时自动回原点，或者预加载生产配方参数。这个过程通常只需几十毫秒，面板上的 RUN 指示灯会快速闪烁提示用户系统正在准备就绪。

3. RUN 模式（运行模式）

这是 PLC 正常工作的“生产状态”。此状态时，PLC 的 CPU 会以毫秒级的间隔（扫描周期）循环执行实时采集现场传感器信号（如光电开关是否被触发）、根据用户编写的逻辑程序（如梯形图）进行计算决策，并输出控制信号驱动执行机构（如启动传送带电机、打开电磁阀）。在此模式下，TIA 博途软件仍可在线监控程序运行，但无法修改程序逻辑，必须切换回 STOP 模式才能进行更改。

PLC 没有机械开关，所有模式切换都通过软件或网络完成。初学者可以通过操作面板指示灯的颜色和状态来快速判断设备状态：绿色常亮表示运行中（RUN）；黄色常亮表示已停机（STOP）；绿色闪烁表示正在启动（STARTUP）；若 ERROR 红灯亮起，表示检测到硬件故障（如模块通信中断）或程序错误（如除零运算），需通过软件查看具体故障代码；MAINT 黄灯亮起则表示需要维护（如电池电量不足或存储卡寿命预警）。

(二) S7-1200 PLC 的循环扫描机制

PLC 的核心工作原理是周期性扫描机制，整个过程就像一个不知疲倦的机器人在流水线上重复三个固定步骤：输入采样，程序执行，输出刷新。

S7-1200 PLC 的扫描工作过程如图 1-3-1 所示。

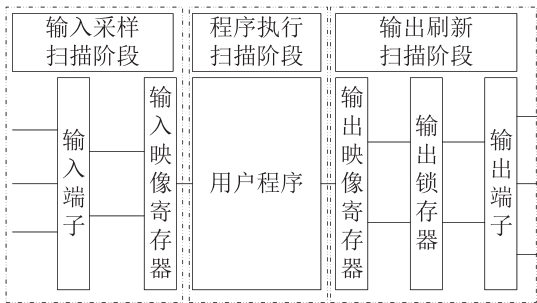


图 1-3-1 S7-1200 PLC 的扫描工作过程

1. 第一阶段：输入采样——收集信号

PLC 以极快速度（微秒级）按顺序扫描所有输入端子（例如 DI0.0~DI0.7），将现场设备的开关量信号（如按钮是否按下）或模拟量数值（如温度传感器的 4~20 mA 信号）统一存入输入映像寄存器（可理解为临时记事本）。信号采集是批量完成的，采集完成后立即“冻结”数据。即使外部信号在后续阶段发生变化，程序本次执行仍使用冻结值。若输入信号持续时间短于扫描周期（例如一个 5 ms 的脉冲信号遇到 10 ms 的扫描周期），则可能导致信号丢失，这种情况需使用高速计数器或中断功能。例如，一个包装机上的光电开关检测到产品通过，这个信号会被记录在输入映像区中，即使产品立即离开导致实际信号消失，程序处理阶段仍认为产品存在，直到下一个扫描周期重新采集。

2. 第二阶段：程序执行——运行控制逻辑

PLC 按用户程序（如梯形图）的编写顺序逐行执行指令，整个过程遵循“先左后右、先上后下”的扫描规则。程序读取的输入数据全部来自输入映像区，而非直接读取物理输入端子。运算中间结果（如计时器当前值、计数器累加数）实时更新到元件映像寄存器，输出指令的结果则暂存到输出映像寄存器，而不是立即驱动外部设备。由于指令执行顺序影响结果，初学者需特别注意逻辑排列。例如若两个网络分别控制同一输出点，最终状态取决于哪条指令最后执行。

此阶段 PLC 的工作过程是：CPU 对用户程序按顺序进行扫描，每扫描到一条指令，就要从输入映像寄存器中读取所需的输入信息状态，而不是直接使用现场的即时输入信息。因为第一个批处理过程（取输入信号状态）已经结束，“大门”已经关闭，现场的即时信号此刻无法进入。对于其他信息，CPU 是从 PLC 的元件映像寄存器中读取。在这个顺序扫描过程中，每一次运算的中间结果都立即写入元件映像寄存器中，这样该元件的状态马上就可以被后续扫描到的指令所利用。因此在编程时，指令的先后位置将决定最后的输出结果。对于输出继电器的扫描结果，CPU 并不是马上去驱动外部负载，而是将其结果写入元件映像寄存器中的输出映像寄存器中，该元件的状态也马上就可以被后面将要扫描到的指令所利用。待整个用户程序扫描阶段结束后，进入输出刷新扫描阶段时，CPU 再成批地将输出信号状态送出去。



在程序执行阶段，即使外部输入信号的状态发生了变化，过程映像输入的状态也不会随之改变，输入信号变化的状态只能在下一个扫描周期的读取输入阶段被读入。执行程序时，对输入/输出的访问通常是通过过程映像，而不是实际的 DO 点，这样做有以下好处。

(1) 在整个程序执行阶段，各过程映像输入点的状态保持不变，程序执行完后再用过程映像输出的值更新输出模块，使系统运行稳定。

(2) 由于过程映像保存在 CPU 的系统存储器中，访问速度比直接访问信号模块快得多。

3. 第三阶段：输出刷新——驱动现场设备

将输出映像寄存器中的批量数据一次性传输到物理输出端子，通过锁存器（数据保持电路）稳定输出信号。输出动作比实际信号变化延迟约 1 个扫描周期，例如扫描周期为 10 ms 时，从按下启动按钮到电机实际运转会有约 10 ms 延迟。假设程序计算出 Q0.0 需要通电，输出刷新阶段会将该信号保持到输出端子，驱动中间继电器吸合，进而控制 380 V 交流接触器启动电机。

（三）S7-1200 PLC 的扫描周期与抗干扰

扫描周期是 PLC 完成一次输入采样、程序执行和输出刷新所需的时间，典型值在 1~100 ms 之间，具体取决于程序复杂度、扩展模块数量和 CPU 型号。普通设备（如传送带、加热炉）对毫秒级延迟不敏感，但高速场景（如同步电机定位、编码器脉冲采集）需使用专用功能：立即 I/O 指令可绕过映像区直接读写物理端口（响应时间 <1 ms），硬件中断通过 OB40 组织块立即响应急停信号，高速输入模块则能记录纳秒级脉冲。

在工程实践中，PLC 的抗干扰设计尤为重要。输入信号通过光耦隔离防止现场电磁干扰损坏 CPU，输出模块提供继电器/晶体管可选类型，继电器型可直接驱动交流负载，晶体管型适合高频脉冲控制。调试时可利用 TIA 博途软件的“监控表”实时查看映像区数据变化，通过“强制”功能临时修改输入信号状态（需谨慎操作），或使用“扫描周期”统计功能优化程序性能。若遇到输出无反应、信号丢失或周期性卡顿等问题，需逐步排查运行模式、映像区数据和硬件连接状态。

通过这种“冻结输入→集中处理→批量输出”的工作机制，既保证了控制逻辑的稳定性，又能通过 S7-1200 灵活的编程，适应从简单的灯光控制到复杂的生产线协调等各种工业场景。理解这些基本原理后，可以更自信地开始梯形图编程和现场调试实践。

任务四

S7-1200 PLC 的编程软件

任务描述

本任务聚焦西门子 S7-1200 PLC 的核心编程软件——TIA 博途 (Totally Integrated Automation Portal)，系统介绍其功能模块、操作流程及在工业控制中的实际应用。TIA 博途作为集成化工程平台，支持 PLC 编程、HMI 组态、驱动配置及网络通信的一体化开发，其模块化设计、高效工程效率和用户友好界面等优势，助力其成为工业自动化领域的标准工具。

任务目标

1. 掌握博途软件集成开发环境，熟练操作编程模块、可视化界面及硬件组态功能，完成 PLC 程序开发到设备联调的全流程实施。掌握硬件模块的即插即用配置方法，实现分布式控制系统搭建与工业通信协议集成。
2. 提升多语言编程与调试能力，灵活运用梯形图、结构化文本等工具开发控制逻辑与算法。通过在线监控与离线仿真工具验证程序准确性，优化工业控制系统的实时响应性能。
3. 构建标准化工程管理体系，制定功能模块命名规范、数据管理规则及代码复用机制。运用协同开发平台实现团队协作与版本控制，规避典型编程错误，强化项目全生命周期管理能力。
4. 践行科技报国使命，通过智能产线开发案例深化产业升级认知，培养严谨的工程思维与工匠精神。探索国产化技术适配路径，增强自主创新意识，主动服务国家智能制造战略需求。

任务实施

一、TIA 博途软件平台解析

博途软件界面如图 1-4-1 所示。作为西门子工业自动化生态的核心载体，TIA Portal (全集成自动化平台) 重构了工程开发范式。该平台通过统一开发环境实现 PLC 编程、人机交互、驱动控制及安全系统的深度集成，覆盖从设备组态到系统联调的完整工



图 1-4-1 高清图



程链条，其标准化工程平台可缩短 40% 以上的开发周期。通过融合 STEP 7、WinCC、Safety 等核心模块，TIA Portal 将传统分散的硬件配置、安全策略制定、HMI 画面设计等任务整合至同一工程界面，支持 PLC 与驱动装置、智能配电设备进行无缝数据交互。

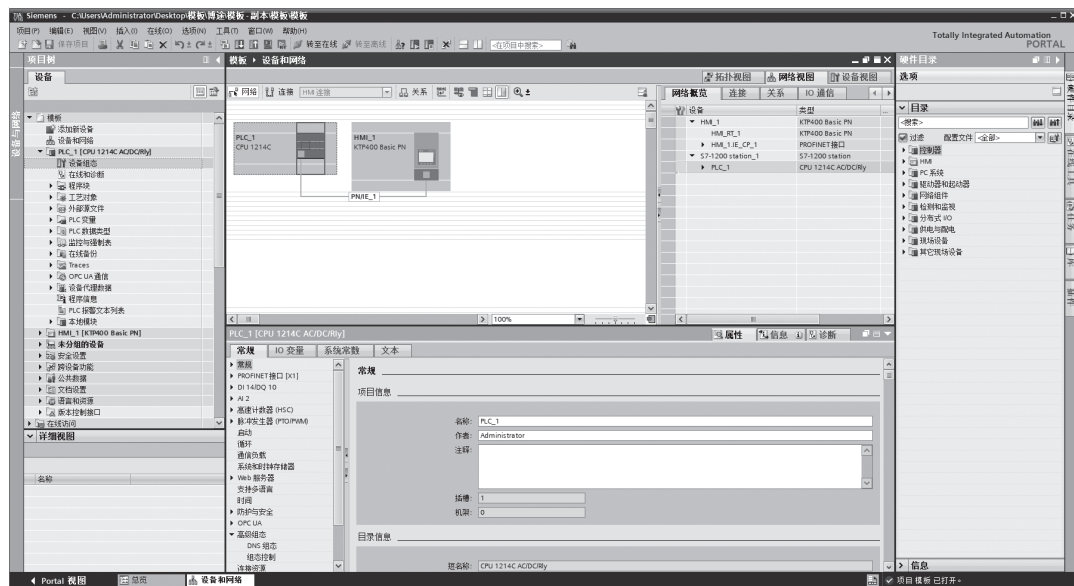


图 1-4-1 博途软件界面

二、模块化功能体系

STEP 7 作为 PLC 工程核心，提供分级开发支持：Basic 版适配 S7-1200 系列基础编程，Professional 版扩展支持 S7-1500/300/400 高端控制器的结构化文本开发。WinCC 人机交互系统采用模块化授权机制：Basic 版实现精简面板基础画面设计，Comfort 版支持精智面板复杂可视化开发，Advanced/Professional 版分别提供 PC 单站与多站分布式系统的 Web 客户端组态能力。Safety 安全套件集成 IEC 61508 认证功能库，实现安全 PLC 的急停、安全门锁等逻辑编程，其安装包与 STEP 7 深度整合，部署效率提升 60%。

三、驱动与仿真扩展

Startdrive 驱动模块打通 PLC 与西门子驱动设备的工程壁垒，支持 G120 变频器、S210 伺服系统的参数化调试与在线诊断，使运动控制系统的组态时间减少 50%。PLCSIM 虚拟调试模块构建数字化验证环境，支持梯形图逻辑测试、变量监控等全功能调试（硬件依赖功能如高速计数、PID 控制需实体设备支持），可在投产前消除 80% 的程序逻辑错误。

四、协同开发优势

平台采用数据联动架构，PLC 变量可通过拖拽直接绑定至 HMI 画面元素，系统自动生成 OPC UA 通信连接，传统需 2 小时完成的通信组态可压缩至 5 分钟。统一工程数据库实现跨设备参数同步，驱动装置配置数据可自动映射至 PLC 控制逻辑，组态错误率

降低 75%。这种高度集成化设计使汽车、制药等行业设备调试效率提升 3 倍以上，正逐渐成为各国工业 4.0 转型的核心工具链。

任务五 S7-1200 PLC 的编程语言

任务描述

本任务旨在通过系统性学习与实践，全面理解西门子 S7-1200 PLC 支持的编程语言体系（包括梯形图 LAD、结构化文本 SCL、功能块图 FBD 及顺序功能图 SFC），深入理解其语法规则、开发逻辑与工业场景适配方法。基于工业自动化需求（如电机启停控制、模拟量信号处理、设备通信集成），灵活运用 LAD 实现电气逻辑还原，完成基础逻辑设计全流程实现。同时，通过工业 4.0 典型场景（如智能产线多设备协同、数据驱动的预测性维护）的实践，培养融合工业物联网、边缘计算等技术的复合型能力。

任务目标

1. 理解 S7-1200 PLC 支持的编程语言类型（梯形图 LAD、功能块图 FBD、结构化文本 SCL、顺序功能图 SFC 等），掌握其语法规则、适用场景及相互调用关系，能够根据控制需求选择合适的语言实现逻辑功能。
2. 能够使用梯形图（LAD）实现基础逻辑控制（如电机启停、互锁保护），通过功能块图（FBD）构建复杂功能模块（如计数器、定时器组合逻辑），并利用结构化文本（SCL）编写算法或数据处理程序（如数学运算、数组操作）。
3. 熟悉顺序功能图（SFC）在流程化控制中的应用（如多工段生产线顺序控制），能够结合多种语言混合编程，优化程序结构并提升代码可维护性。
4. 在编程实践中强化代码规范性（如变量命名、注释标准化）与工程伦理意识，理解标准化编程在系统可靠性和团队协作等方面的重要意义，树立技术创新与安全生产并重的职业理念。

任务实施

一、核心编程语言支持与功能特性

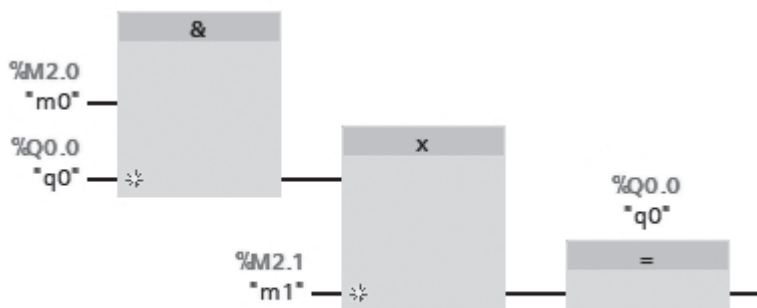
西门子 S7-1200 PLC 基于 IEC61131-3 标准，支持梯形图（LAD）、功能块图（FBD）



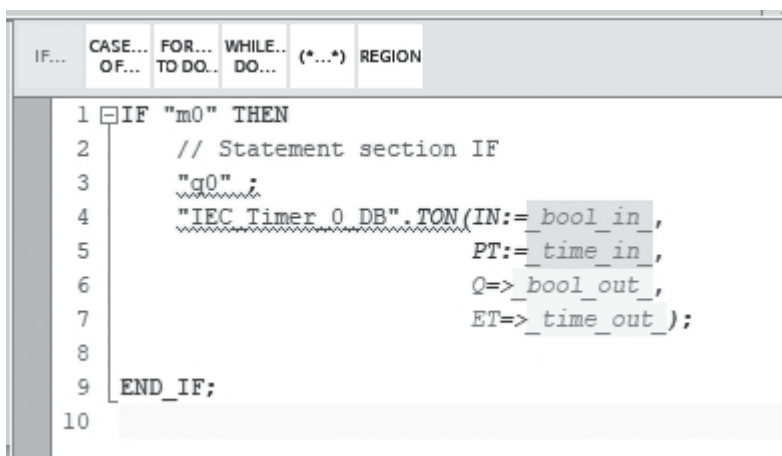
和结构化文本 (SCL) 三种核心编程语言。三种语言对比如图 1-5-1 所示。梯形图 (LAD) 采用继电器逻辑符号构建控制逻辑，直观模拟电流“能流”特性，适用于电机启停、传感器连锁等基础场景，其开发效率比传统继电器系统提升超过 40%；功能块图 (FBD) 通过图形化模块（如 AND/OR 门、定时器）实现组合逻辑和数学运算，适合多信号连锁及标准化模块封装（如 PID 控制）；结构化文本 (SCL) 作为高级文本语言，支持复杂算法（如数据滤波、运动控制）和配方管理，其代码执行效率比 LAD 提升 50%，尤其在循环运算和条件分支处理中表现突出。



梯形图 (LAD)



功能块图 (FBD)



结构化文本 (SCL)

图 1-5-1 S7-1200 PLC 三种语言对比

二、开发环境与工具集成

所有编程均在 TIA Portal 平台完成，该环境深度融合工程管理、调试和仿真功能。开发者可在同一项目中混合使用 LAD、FBD 和 SCL 语言，并通过全局变量表统一管理数据地址，避免硬件冲突；调试工具支持在线监控变量状态、设置断点及交叉引用分析，PLC SIM 模块允许无硬件条件下验证程序逻辑（注：高速计数等硬件功能需实体设备支持）；平台内置工艺库（如 PID_Compact）和用户自定义函数块（FB）功能，支持快速调用标准算法模块，同时提供数据类型自动校验（如 INT 与 REAL 类型匹配），显著降低编程错误率。

三、不支持的语言与替代方案

S7-1200 受硬件资源限制（如 CPU 处理能力），不支持顺序功能图（SFC）和语句表（STL）。对于需多状态流程控制的场景，可通过 SCL 编写状态机逻辑（如 CASE 语句实现工序跳转）或 LAD 中的置位 / 复位指令模拟步序控制；STL 的功能可完全由 SCL 替代，后者代码可读性更优且兼容性更强。此外，LabVIEW 等图形化语言需通过 Profinet/OPCUA 协议与 PLC 交互，无法直接嵌入 TIA Portal 开发环境。

四、语言选择策略与优化建议

针对不同场景推荐语言组合：简单逻辑（如设备启停）优先使用 LAD 以缩短开发周期；复杂运算（如模糊控制）采用 SCL 编写函数块，可减少 30% 代码量；模块化设计（如报警管理）使用 FBD 封装标准化功能块。优化实践包括：高频变量使用 DWORD 类型提升处理速度（比 BOOL 组快 20%）、分离控制逻辑（OB1）与数据处理逻辑（FB/FC）以提升可维护性、避免循环中频繁调用大型函数块防止扫描周期波动。

五、与其他 PLC 系列的对比与升级建议

相比于 S7-1500 系列，S7-1200 缺少 SFC 编程和多任务处理能力，但其性价比在中小型设备（如包装机、流水线）中占据优势；S7-1500 支持 G 代码解析和 1 MHz 高速脉冲输出，适用于复杂运动控制（如机械手轨迹规划）。与 S7-300/400 系列相比，S7-1200 仅兼容 TIA Portal 开发环境，而后者需 STEP 7 Classic 软件且适合大型冗余系统。对于需多工序并行（如化工反应釜）或超高速响应（扫描周期 <1 ms）的场景，建议升级至 S7-1500 系列以获取更全面的功能支持。