第一部分　概述篇

项目 1　认识 S7-1200 PLC

1.1　S7-1200 PLC 简介

西门子 PLC 以其极高的性价比，在国内外占有很大的市场份额，在我国得到了广泛的应用。

S7-1200 PLC 控制器是西门子系列 PLC 的新产品，因其设计紧凑、组态灵活、扩展方便、功能强大，可用于控制各种各样的设备以满足自动化需求。S7-1200 CPU 模块将微处理器、集成电源、输入和输出电路、内置 PROFINET、高速运动控制 I/O、多种工艺功能及模拟量输入组合到一个设计紧凑的外壳中，形成功能强大的控制器，这些特点的组合使它成为各种控制应用中完美的解决方案。由于 S7-1200 PLC 在西门子 PLC 家族中属于模块化小型 PLC，因此适用于各种中低端独立式自动化系统中，如图 1-1 所示。

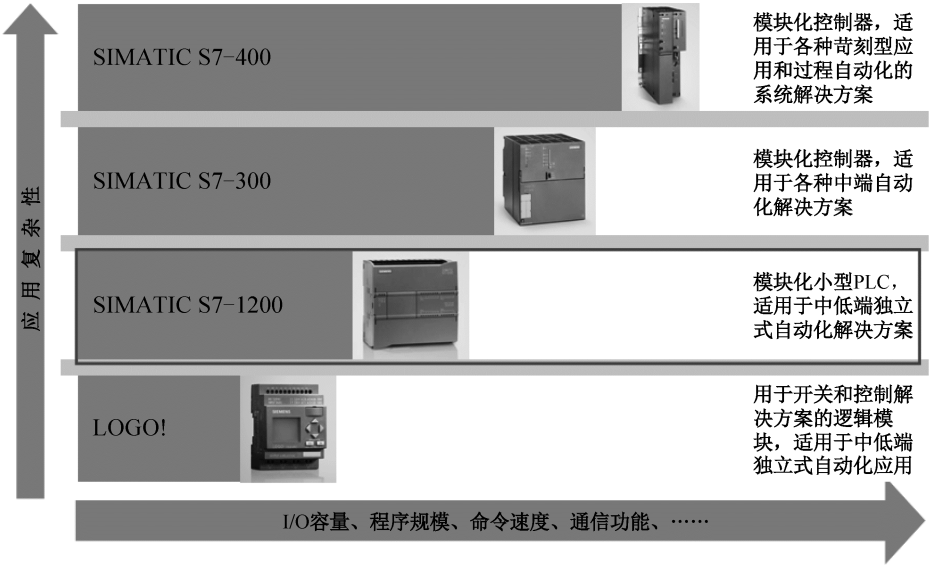
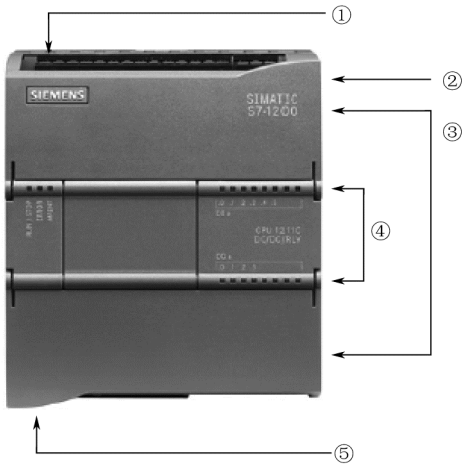


图 1-1　S7-1200 PLC 的应用定位

S7-1200 PLC 的外形如图 1-2 所示，CPU 提供一个 PROFINET 端口实现与编程计算机、人机界面、其他 PLC 及带以太网接口的设备进行通信。还可使用附加模块通过 PROFIBUS、GPRS、RS485 或 RS232 等进行通信。



1—电源接口；2—存储卡插槽（上部保护盖下面）；3—可拆卸用户接线连接器（保护盖下面）；
4—板载 I/O 的状态 LED；5—PROFINET 连接器（CPU 的底部）

图 1-2　S7-1200 PLC 外形

S7-1200 PLC 目前有 4 种 CPU 型号，分别为 CPU1211C、CPU1212C、CPU1214C、CPU1215C。各种型号的参数比较如表 1-1 所示。

表 1-1　S7-1200 PLC 各种型号参数比较

CPU 的功能	CPU1211C	CPU1212C	CPU1214C	CPU1215C
本机数字量输入输出 本机模拟量输入输出	6 输入/4 输出 2 输入	8 输入/6 输出 2 输入	14 输入/10 输出 2 输入	14 输入/10 输出 2 输入/2 输出
扩展模块个数	-	2	8	8
高速计数器	3（总计）	4（总计）	6（总计）	6（总计）
集成/可扩展的 工作存储器 集成/可扩展的 装载存储器	25KB/不可扩展 1MB/24MB	25KB/不可扩展 1MB/24MB	50KB/不可扩展 2MB/24MB	100KB/不可扩展 2MB/24MB
单相计数器	3 个 100kHz	3 个 100kHz 和 1 个 30kHz	3 个 100kHz 和 3 个 30kHz	3 个 100kHz 和 3 个 30kHz
正交计数器	3 个 80kHz	3 个 80kHz 和 1 个 30kHz	3 个 80kHz 和 3 个 30kHz	3 个 80kHz 和 3 个 30kHz
脉冲输出	两个 100kHz（DC 输出）或两个 1Hz（RLY 输出）			
脉冲同步输入	6	8	14	14
延时/循环中断	总计 4 个，分辨率 1ms			
边沿触发式中断	6 个上升沿和 6 个下降沿	8 个上升沿和 8 个下降沿	12 个上升沿和 12 个下降沿	12 个上升沿和 12 个下降沿
实时时钟精度	±60s/月			
PROFINET	1 个以太网通信口			2 个以太网通信口
实时时钟保持时间	典型 10 天/最低 6 天，40℃时			
数学运算执行速度	2.3μs/指令			
布尔运算执行速度	0.08μs/指令			

1.2 S7-1200 PLC 的程序结构和工作原理

1．S7-1200 PLC 的程序结构

S7-1200 PLC 与 S7-300/400PLC 的程序结构基本相同，都采用模块化编程。S7-1200 PLC 用户程序中的块包括组织块（OB）、功能块（FB）、功能（FC）和数据块（DB），其中数据块又包括背景数据块和全局数据块两种，模块化的程序结构，易于程序的阅读、调试与维护，可移植性强。用户程序块见表 1-2 所示。

表 1-2 用户程序块

块	描述
组织块（OB）	操作系统与用户程序之间的接口，用户可以对组织块编程
功能块（FB）	用户编写的包含经常使用的功能的子程序，有专用的背景数据块
功能（FC）	用户编写的包含经常使用的功能的子程序，没有专用的背景数据块
背景数据块（DB）	用于保存 FB 输入变量、输出变量和静态变量，其数据在编译时自动生成
全局数据块（DB）	存储用户数据的数据区，供所有程序享用

1）组织块

操作系统与用户程序之间的接口，用户可以对组织块编程，据此可以明确定义 CPU 的响应行为。组织块由操作系统调用，用于处理以下事件：启动行为、循环程序执行、中断驱动的程序运行及错误处理，相应的有启动组织块、循环组织块和中断组织块。

（1）启动组织块：在运行模式从 STOP 切换为 RUN 运行时，启动组织块用来初始化程序中的变量，启动组织块运行结束之后，开始运行循环组织块。

（2）循环组织块：循环组织块是程序中的较高层程序块，可以调用其他块。OB1 是用户程序中的主程序，允许有多个循环组织块，但编号应大于等于 200。CPU 按照循环组织块的编号，从小到大循环执行循环组织块。

（3）中断组织块：中断组织块用来对内部或外部事件做出快速反应，如果出现中断事件，将执行中断组织块，中断组织块包括延时中断组织块（Time Delay Interrupt）、循环中断组织块（Cyclic Interrupt）、硬件中断组织块（Hardware Interrupt）、诊断错误中断组织块（Diagnostic Error Interrupt）和时间错误中断组织块（Time Error Interrupt）。

① 延时中断组织块：在指定的时间过后，执行中断循环程序，延时时间通过扩展指令“SRT_DINT”的输入参数指定。

② 循环中断组织块：在特定的时间段，执行中断循环程序，通过对话框或者组织块的属性可以指定该类时间段。

③ 硬件中断组织块：根据硬件事件触发，执行中断循环程序，事件在硬件属性中定义。

④ 诊断错误中断组织块：在具备诊断功能的模块已经被启用诊断中断并检测到错误时，执行中断循环程序。

⑤ 时间错误中断组织块：在超过了最大循环时间时，执行中断循环程序，最大循环时间在 CPU 的属性中定义。

2）功能

功能（FC）是用户编写的一种可以快速执行的子程序块，通常用于根据输入参数执行指令。使用 FC 可以完成以下任务：① 创建一个可重复使用的操作，如公式计算；② 创建一个可重复使用的技术工艺功能，如阀门控制。在程序中的不同点可以多次调用 FC。FC 没有分配给它的数据块。FC 使用临时堆栈临时保存数据。FC 退出后，临时堆栈中的变量将丢失。要长期存储数据，可将输出值赋给全局存储器，如 M（位）存储器或全局数据块 DB。

3）功能块

功能块（FB）也是用户编写的一种使用参数进行调用的程序块。其参数存储在局部数据块（背景数据块）内。FB 退出运行之后，保存在背景数据块内的数据不会丢失。FB 可以多次调用。每次调用都可以分配一个独立的背景数据块，多个独立的背景也可以组合成一个多重背景数据块。

4）数据块

数据块用于保存用户数据，数据块的最大大小由 CPU 的工作存储器决定。它分为全局数据块和背景数据块两种。用户程序中的所有程序块都可访问全局 DB 中的数据，而背景 DB 仅存储特定功能块（FB）的数据，背景 DB 中数据的结构反映了 FB 的参数（Input、Output 和 InOut）和静态数据，但 FB 的临时存储器不存储在背景 DB 中。

综上所述，S7-1200 PLC 的程序结构框图如 1-3 所示。

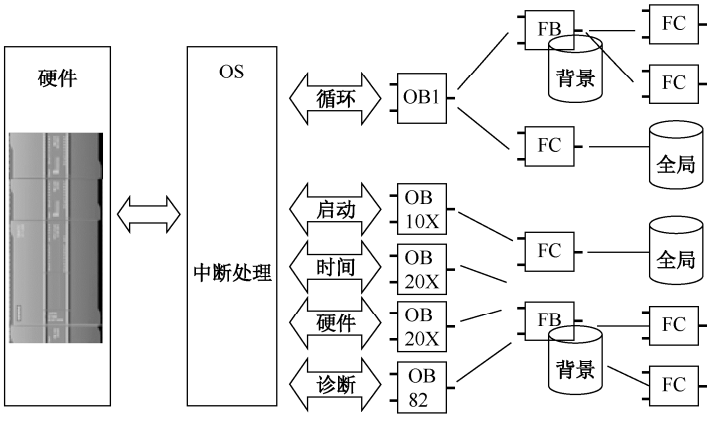


图 1-3　S7-1200 PLC 的程序结构框图

2．PLC 工作原理

1）CPU 的工作模式

CPU 有 3 种工作模式：STOP 模式、STARTUP 模式和 RUN 模式，CPU 前面的状态 LED 指示当前工作模式。

（1）在 STOP 模式下 CPU 不执行程序，所有的输出被禁止或按组态时的设置提供替代值或保持最后的输出值，以保证系统处于安全状态，在 STOP 模式下才可以下载项目。

（2）在 STARTUP 模式下执行一次启动 OB（如果存在），在 STARTUP 模式下不处

理任何中断事件。若系统检测到某种错误，CPU 将不能进入 RUN 模式，并保持在 STOP 模式。

（3）在 RUN 模式下会重复执行程序循环 OB，任何时刻都可能发生中断事件并对其进行处理。CPU 支持通过暖启动进入 RUN 模式。暖启动不包括储存器复位，在暖启动时，所有非保持性系统及用户数据都将被初始化，保留保持性用户数据。存储器复位将清除所有工作存储器、保持性及非保持性存储区，并将装载存储器复制到工作存储器。存储器复位不会清除诊断缓冲区，也不会清除永久保存的 IP 地址值。

可组态 CPU 中“上电后启动”（Start Up after POWER ON）设置。该组态项出现在 CPU“设备组态”（Device Configuration）的“启动”（Start Up）下，通电后，CPU 将执行一系列上电诊断检查和系统初始化操作，在系统初始化过程中，CPU 将删除所有非保持性位存储器，并将所有非保持性 DB 的内容重置为装载存储器的初始值。CPU 将保留保持性位存储器和保持性 DB 中的内容，然后切换到相应的工作模式。检测到的某些错误会阻止 CPU 进入 RUN 模式。

CPU 支持的组态选项有不重新启动（保持为 STOP 模式）、暖启动（RUN 模式）、暖启动（断电前的模式）。

可以使用编程软件在线工具中的“STOP”或“RUN”命令更改当前工作模式，也可在程序中包含 STP 指令，以使 CPU 切换到 STOP 模式。这样就可以根据程序逻辑停止程序的执行。

在 STARTUP 和 RUN 模式下，CPU 执行如图 1-4 所示的任务。

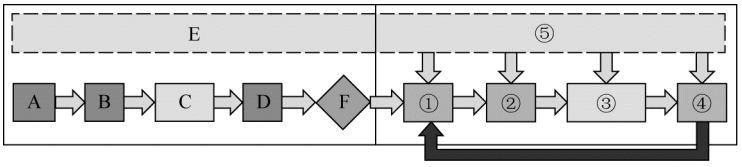


图 1-4　CPU 执行的任务

STARTUP	RUN
A 清除 I（映像）存储区	①将 Q 存储器写入物理输出
B 使用上一个值或替换值对输出执行初始化	②将物理输入的状态复制到 I 存储器
C 执行启动 OB	③执行程序循环 OB
D 将物理输入的状态复制到 I 存储器	④执行自检诊断
E 将所有中断事件存储到要在进入 RUN 模式后处理的队列	⑤在扫描周期的任何阶段处理中断和通信
F 启用	Q 存储器到物理输出的写入操作

2）STARTUP 过程

只要工作模式从 STOP 切换到 RUN 模式，CPU 就会清除过程映像输入、初始化过程映像输出，并处理启动 OB。通过“启动 OB”中的指令对过程映像输入寄存器进行任何的读访问，都只会读取零值，而不是读取当前物理输入值。因此，要在启动模式下读取物理输入的当前状态，必须执行立即读取操作，接着再执行启动 OB 及任何相关的 FC 和 FB。如果存在多个启动 OB，则按照 OB 编号依次执行各启动 OB，OB 编号最小的先执行。

3）在 RUN 模式下处理扫描周期

在每个扫描周期中，CPU 都会写入输出、读取输入、执行用户程序、更新通信模块及响应用户中断事件和通信请求，在扫描期间会定期处理通信请求。以上操作（用户中断事件除外）按先后顺序定期进行处理，对于已启用的用户中断事件，将根据优先级按其发生顺序进行处理。系统要保证扫描周期在一定的时间段内（即最大循环时间）完成，否则将生成时间错误事件。

在每个扫描周期的开始，从输出过程映像寄存器重新获取数字量及模拟量输出的当前值，然后将其写入到 CPU、SB 和 SM 模块上，自动 I/O 更新（默认组态）的物理输出。通过指令访问物理输出时，输出过程映像寄存器和物理输出本身都将被更新。

随后在该扫描周期中，将读取 CPU、SB 和 SM 模块上组态为自动 I/O 更新（默认组态）的数字量及模拟量输入的当前值，然后将这些值写入输入过程映像寄存器。通过指令访问物理输入时，指令将访问物理输入的值，但输入过程映像不会更新。

读取输入后，系统将从第一条指令开始执行用户程序，一直执行到最后一条指令。其中包括所有的程序循环 OB 及其所有关联的 FC 和 FB。程序循环 OB 是根据 OB 编号依次执行，OB 编号最小的先执行。

在扫描期间会定期处理通信请求，这可能会中断用户程序的执行。自诊断检查包括定期检查系统和检查 I/O 模块的状态。中断可能发生在扫描周期的任何阶段，并且由事件驱动，事件发生时，CPU 将中断扫描循环，并调用被组态用于处理该事件的 OB。OB 处理完该事件后，CPU 从中断点继续执行用户程序。

1.3　CPU 的扩展功能

1．信号板

CPU 支持一个插入式扩展板，即信号板（SB），信号板可为 CPU 提供附加 I/O，安装后不会改变 CPU 的外形和体积。信号板有 8 种型号，包括一点模拟量输出、两点数字量输入/输出及 6 种 200kHz 的数字量输入和数字量输出信号板。图 1-5 为信号板的外形。

图 1-5　信号板的外形

2．信号模块

信号模块（SM）可以为 CPU 增加其他功能，SM 连接在 CPU 右侧，分为数字量 I/O、模拟量 I/O、RTD 和热电偶信号模块。

数字量输入/输出模块（DI/DO）可以选 8 点、16 点和 32 点，如表 1-3 所示。

表 1-3　数字量输入/输出模块

型号	各组输入点数	各组输出点数
SM1221，8 输入，DC24V	4,4	
SM1221，16 输入，DC24V	4,4,4,4	
SM1222，8 继电器输出，2A		3,5
SM1222，16 继电器输出，2A		4,4,2,6
SM1222，8 输出，DC24V，0.5A		4,4
SM1222，16 输出，DC24V，0.5A		4,4,4,4
SM1223，8 输入 DC24V/8 继电器输出，2A	4,4	4,4
SM1223，16 输入 DC24V/16 继电器输出，2A	8,8	4,4,4,4
SM1223，8 输入 DC24V/8 输出 DC24V，0.5A	4,4	4,4
SM1223，16 输入 DC24V/16 输出 DC24V，0.5A	8,8	8,8

模拟量模块包括 4 路模拟量输入模块（如 SM1231AI）和 8 路模拟量输入模块，模块的输入电压可以选择−10～+10V、−5～+5V、−2.5～+2.5V，转换后对应数字量为−27648～+27648；电流为 0～20mA，转换后对应数字量为 0～27648；2 路模拟量输出模块（如 SM1232AQ）和 4 路模拟量输出模块，输出电压为−10～+10V，对应数字量为−27648～+27648，输出电流为 0～20mA，对应的数字量为 0～27648。4 路模拟量输入/2 路模拟量输出模块（如 SM1234AI/AQ），其参数与模拟量输入、模拟量输出参数相同。此外，还有热电偶、热电阻模拟量测量模块。

3．通信模块

通信模块（CM）增加了 CPU 的通信选项，如 PROFIBUS 或 RS232/RS485 的连接性（适用于 PtP、Modbus 或 USS）或者 AS-i 主站。CP 可以提供其他类型的通信功能，如通过 GPRS 网络连接 CPU。CPU 最多支持 3 个 CM，并且要求安装在 CPU 的左侧。

4．S7-1200 PLC 新模块

各种新模块扩展了 S7-1200 CPU 的功能，因而能够灵活地满足自动化需要，新的和改进的 CPU 包括以下几种。

（1）新的 CPU1215CDC/DC/DC、CPU1215CDC/DC/继电器和 CPU1215CAC/DC/继电器提供了 100KB 的工作存储器、双以太网和模拟量输出。

（2）新的和改进的 CPU1211C、CPU1212C 和 CPU1214C 具有更短的处理时间、可使用 4 个 PTO（CPU1211C 需要信号板）、更大的保持性存储器（10KB）及更长的保持时间（20 天）。

（3）内置 PROFINET 接口：用于编程、HMI 连接和 CPU 之间的通信。通过开放式以太网

协议，与第三方设备进行通信，最多支持 8 个以太网连接，通信组态可以采用 STEP7 命令“T-Send/T-Receive”完成，从固件版本 2.0 开始，用于控制器/设备的 PROFINETIO 功能。

5．集成技术

集成技术用于计数和测量：设计有多达 6 个高速计数器。其中，3 个工作频率为 100kHz，3 个工作频率为 30kHz；用于准确地监控增量编码器和过程事件的频率计数或者高速计数功能；用于控制速度、位置和标记占空比，总共有 2 路 PWM（脉宽调制）输出，应用实例包括电机速度控制、阀门位置控制或者加热元件占空比控制；用于速度和位置控制，总共有 2 路 PTO 输出 100kHz（脉冲串输出）提供有一个脉冲串；用于控制步进或者伺服电机的速度和位置，PLCopen 是国际公认的运动控制标准支持绝对、相对和速度控制及运动控制中切换功能。

它还可实现简单的过程仪表和控制：高达 16 个 PID 控制循环，支持 PID 自动调节功能，带有调节控制面板。

1.4　PLC 应用技术技能型人才培养

1．PLC 应用技术的岗位需求

作为现代工业自动化三大支柱的核心技术之一的 PLC 技术，已综合了计算机控制技术、自动控制技术和网络通信技术，其应用于系统过程控制、运动控制、网络通信、人机交互等各个领域。基于对更高自动化程度和更高能效的需要，尤其是制造业会越来越多地应用 PLC，在制造过程中，以最低生产设备生命周期成本来实现适应性和灵活性的日益增加的需求，给 PLC 技术应用提供了不竭的动力。西门子公司的 PLC 在我国的应用也相当广泛，1996 年，随着西门子公司提出的 TIA（Totally Integrated Automation）概念，即全集成自动化系统，将 PLC 技术融于全部自动化领域，它具有开放系统的基本结构，扩展方便，是解决自动化任务的一套全新的方法。而 S7 系列 PLC 发展成为了西门子自动化系统的控制核心，它是西门子自动化系统最尖端，功能最强的可编程控制器。因此，不但 PLC 的从业人员，很多工程技术人员都必须掌握 PLC 的操作应用和设计开发能力，以适应不断革新技术。而西门子公司的 PLC 在市场的占有率高，在企业广泛应用，因此学习西门子 PLC 不失为是一个好的选择。

2．PLC 应用技术的岗位能力

PLC 应用技术工作人员要求从事可编程序控制器（PLC）选型、编程，并对应用系统进行设计、集成和运行管理的人员。其岗位能力主要体现在以下几个方面。

（1）以 PLC 为核心的电气控制设备的识图、安装、调试能力。

（2）PLC 系统整体集成、系统维护与故障诊断能力。

（3）PLC 系统程序设计、调试能力。

（4）PLC 与 PLC、HMI、变频器、上位机等网络通信能力。

（5）现场总线与工业以太网构建能力。

（6）PLC 应用系统的工艺规程编制和技术文档的编写能力。

3．PLC 应用技术的课程设计

PLC 应用技术是电气自动化技术、机电一体化技术等电类专业的核心技术，课程设计需要体现工作过程的职业岗位能力需求。PLC 在企业生产实践中的应用不是孤立的，而是综合了机械技术、传感检测技术、电机驱动技术、气动控制技术、网络通信技术和人机界面等技术构成的一个完整的自动化生产线，体现全集成自动化系统的概念。因此，PLC 应用技术课程的设计包括以小型 S7-1200 PLC 为载体的基础应用、以中型 S7-300 PLC 为载体的综合应用及以大型 S7-400 PLC 为载体的自动化生产线的系统应用三大模块，通过三大模块的系统学习和实践，以培养 PLC 的系统应用和综合创新能力。

4．PLC 应用技术的行业培训与职业标准

一方面，本书采用了西门子公司最新推出的全新小型自动化解决方案的最佳控制器 S7-1200 PLC，以西门子培训认证内容为背景；另一方面，作者进行了广泛的 PLC 应用领域（自动化生产线、电气控制技术设备等）调研，与企业高级工程师、高级技术人员、一线的技术工人进行反复沟通，并由电气自动化技术专业的企业专业带头人进行详细的指导将 PLC 应用技术的岗位任务进行学习领域的设计。引入了“行业引领”“能力本位”“需求导向”“学生中心”等理念，以全面素质为基础，以能力为本位，把提高职业能力放在突出的位置，以满足 PLC 技术应用型人才培养的要求。因此，本书是在西门子 STPA02：“SIMATIC S7-1200 System Course”课程认证培训内容的基础上，按照基于工作过程核心技术一体化的思路，编写的一本即适合工程技术人员自学，又满足高职高专机电设备类、自动化类专业的项目化教材。

5．学习资源

PLC 的教学资料可以在西门子（中国）有限公司工业业务领域自动化与驱动技术集团的中文网站下载，网址：www.ad.siemens.com.cn 进入该网站的“支持中心”后，在技术资源库的“下载中心”即可找到相应的中英文使用手册，产品样本、常见问题及软件。