

# 西门子工业低压开关经销总代理商

产品名称	西门子工业低压开关经销总代理商
公司名称	浔之漫智控技术（上海）有限公司-西门子模组
价格	.00/件
规格参数	西门子:PLC 模块:经销商
公司地址	213室
联系电话	13817547326

## 产品详情

西门子工业低压开关经销总代理商6. 重新启动 HMI 运行系统软件。精智面板，第二代移动面板1. 通过 Windows CE 桌面图标“ My Device ”，打开文件管理器。2. 浏览到目录“ \flash\simatic\SystemRoot\OMS\Untrusted ”。该 CPU 的 PLC 通信证书位于该目录中。3. 将该 CPU 的 PLC 通信证书复制到目录“ \flash\simatic\SystemRoot\OMS\Trusted ”中。4. 重新启动 HMI 运行系统软件。如果该 PLC 通信证书在 HMI 设备中的状态已标记为“ 可信 ”，则可建立 HMI 安全通信。更多信息，请参见 HMI 设备的操作说明。5.6.5.6 在 TIA Portal 中使用传统的 PG/PC 通信在 TIA Portal V17 及以上版本中，TIA Portal 支持与 S71200/S71500 CPU 固件版本 V4.5/V2.9及以上版本自动进行“ 安全 ”通信。即，连接伙伴自动将各自的连接机制设置为所支持的最高安全连接方式。仅在特定条件下（参见“ 兼容性相关信息 (页 95) ”），才会回退为原 PG/PC 通信方式，即“ 传统的 PG/PC 通信 ”。如果 CPU 的通信性能较差，而高安全性会影响该 CPU 传输速率。此时可能无需采用较高安全性。要求 CPU 间未建立在线连接。如果对 CPU 进行在线访问，则需禁用“ 仅支持 PG/PC 和 HMI 安全通信 ” (Only permit securePG/PC and HMI communication) 选项（“ 连接机制 ” (Connection mechanisms) 区域中的 CPU 参数）。通信伙伴位于受保护环境，如调试阶段。设置传统的 PG/PC 通信1. 在“ 在线 ” (Online) 菜单中，选择命令“ 仅使用传统的 PG/PC 通信 ” (Use only Legacy PG/PC communication)。2. 选择该菜单命令前的复选框。结果：TIA Portal V17 以下版本均建立在线连接。在会话期间，该设置始终有效。项目打开时，“ 仅使用传统的 PG/PC 通信 ” (Use only · legacyPG/PC communication) 选项未设置。

工控机等工业自动化的设计、技术开发、项目选型安装调试等相关服务是专业从事工业自动化控制系统、机电一体化装备和信息化软件系统

集成和硬件维护服务的综合性企业。与西门子品牌合作，只为能给中国的客户提供值得信赖的服务体系，我们

的业务范围涉及工业自动化科技产品的设计开发、技术服务、安装调试、销售及配套服务领域。建立现代化仓

储基地、积累充足的产品储备、引入万余款各式工业自动化科技产品，我们以持续的卓越与服务，取得了年销

售额10亿元的佳绩，凭高满意的服务赢得了社会各界的好评及青睐。其产品范围包括西门子S7-SMART200、S7-200CN、S7-300、S7-400、S7-1200、S7-1500、S7-ET200SP等各类工业自动化产品。西门子授权代理商、西门子一级代理商、西门子PLC模块代理商，西门子模块代理商供应全国范围：

与此同时，我们还提供。

西门子中国授权代理商——浔之漫智控技术（上海）有限公司，本公司坐落于松江工业区西部科技园，西边和全球zhuming芯片制造商台积电毗邻，

东边是松江大学城，向北5公里是佘山国家旅游度假区。轨道交通9号线、沪杭高速公路、同三国道、松闵路等

交通主干道将松江工业区与上海市内外连接，交通十分便利。

目前，浔之漫智控技术（上海）有限公司将产品布局于中、高端自动化科技产品领域，

PLC模块S7-200、S7-1200、S7-300、S7-400、ET200分布式I/O等

HMI触摸屏、SITOP电源、6GK网络产品、ET200分布式I/O SIEMENS 驱动产品MM系列变频器、G110 G120变频器、直流调速器、电线电缆、

驱动伺服产品、数控设备SIEMENS低压配电与控制产品及软启动器等

启用“仅使用传统的PG/PC通信”（Use only · Legacy PG/PC communication）选项时的特性 CPU 中保护机密 PLC 组态数据的密码无法在线指定、修改或删除。需要禁用“仅使用传统的PG/PC通信”（Use only · Legacy PG/PC communication）选项才能使用上述功能。设置为仅支持PG/PC和HMI安全通信的CPU无法在线访问。5.6.5.7兼容性相关信息下文中介绍了不同TIA Portal版本与不同CPU固件版本间的相互关系以及对PG/HMI连接类型的影响。使用TIA Portal V17

以下版本创建的项目例如，如果使用TIA Portal V16创建适用于S7-1500 CPU（例如，版本V2.8）的项目，也可以将使用TIA Portal V17实现的相应组态下载到S7-1500 CPU V2.9中，例如，在备件方案中 - 与S7-1500 CPU V2.8上的组态具有相同的行为。对于使用TIA Portal V17以下版本创建并传送到存储卡的项目，在S7-1500 CPU V2.9中也可以正常运行。但是，使用TIA Portal V17及以上版本打开项目，通过更换设备来更新CPU的固件版本，并借此将其保存为固件版本为V2.9及以上版本的CPU后，就会立即应用保护机密PLC组态数据的概念（参见“有关保护机密PLC组态数据的实用信息（页64）”）。不可再使用低于TIA Portal V17的版本编辑该项目。PG/HMI和CPU的连接方式不同如前几节所述，在V17及以上版本中，PG/HMI设备与CPU（最新版本）之间的安全PG/HMI连接的优势在于采用标准化通信程序TLS（传输层安全）。可以选择将V2.9 CPU连接到装有TIA Portal V17或更高版本的最新编程设备，此外，还可以连接到装有早期运行系统版本的HMI设备：设备会相应地自动调整其连接机制。为了能够更好地区分这两种连接机制，我们将先前的程序为“传统方式”（基于S7通信的升级版）。概括地说（此处“PG”代表装有TIA Portal的编程设备）：PG/HMI和CPU随V17（或后续版本）提供：使用TLS程序。PG/HMI的版本为旧版本（< V17）：使用传统方式 - 前提是已取消激活CPU属性中的选项“仅允许PG/PC和HMI间安全通信”（Only allow secure PG/PC and HMI communication）。CPU随V17（或更高版本）提供，连接的多个PG/HMI来自V17（或更高版本）和以前的版本：使用TLS + 传统方式 - 前提是已取消激活CPU属性中的选项“仅允许PG/PC和HMI间安全通信”（Only allow secure PG/PC and HMI communication）。当CPU状态改变时如果CPU状态因PG/HMI

间安全通信相关事件而发生改变，则诊断缓冲区会向用户提供相关信息。示例：  
成功下载包含已组态密码的组态后，诊断缓冲区将报告 CPU 正在从配置阶段切换为安全模式（TLS 程序）。已将装有 TIA Portal V17 的 PG 连接到 CPU V2.9。若“在线”（Online）菜单中禁用“仅使用传统的 PG/PC 通信”，将自动建立 PG/HMI 间安全通信（TLS 程序）。有关设备或固件特性（如使用的 TLS 版本）的信息，请参见“设备相关的安全功能（页 47）”部分。

5.7 SNMP 5.7.1 激活和取消激活 SNMP 网络管理协议 SNMP (Simple Network Management Protocol) 用于对网络拓扑进行监视和诊断。SNMP 采用传输协议 UDP 并具有两个角色：SNMP 管理器（客户端）和 SNMP 代理（服务器）。SNMP 管理器用于对网络节点进行监视；SNMP 代理则收集各个网络节点的各种网络特定信息，并以结构化的形式存储在 MIB (Management Information Base) 中。多种服务和工具（作为 SNMP 管理器）以这些数据为基础执行详细的网络诊断。SNMP 还适用于 PROFINET IO 系统，用于管理网络基础设施以及 IO 控制器/IO 设备。说明如果取消激活设备的 SNMP 功能，则无法使用各种网络拓扑诊断选项（例如，使用 PRONETA 工具）。示例：对于在线-离线拓扑比较，TIA Portal 确定实际连接的端口并将 SNMP 用于此功能。默认设置取决于固件版本 S7-1500 CPU 已集成 SNMP 代理。SNMP 采用不同的默认设置（SNMP 激活或取消激活），与具体的固件版本有关。对于固件版本低于 V3.0 的 S7-1500 CPU，SNMP 代理默认情况下激活，仅可在用户程序中通过数据记录取消激活。在某些特定条件下，可能需要取消激活 SNMP。示例：网络中的安全规则不允许使用 SNMP。用户可使用自己的通信指令，定制相应的 SNMP 解决方案。对于固件版本为 V3.0 的 S7-1500 CPU，SNMP 代理默认情况下取消激活。如果未下载组态或未插入存储卡，将采用默认设置“已取消激活”。对于固件版本为 V3.0 或更高版本的 S71500 CPU，STEP 7 V18 可通过以下方式更改 SNMP 设置：在 TIA Portal 的 CPU 属性中组态 SNMP。通过向 PROFINET 接口传送数据记录在用户程序中激活/禁用 SNMP。说明更换部件方案出于兼容性原因，固件版本为 V3.0 及以上版本的 S7-1500 CPU，如果下载了低版本项目（CPU 固件 < V3.0），其行为与低版本项目中的 CPU 类似：SNMP 已激活，“public”和“private”社区字符串生效。自 CPU 固件版本 V3.0 以及 TIA Portal V18 起，可在 CPU 属性中更改以下 SNMP 设置：激活 SNMP（默认设置：已取消激活）只读团体字符串（默认值：“public”）读写团体字符串（默认值：“private”）相关设置，请参见“gaoji 组态 > SNMP” (Advanced configuration > SNMP) 区域。从 CPU 固件版本 V3.1 和 TIA Portal 版本 V19 开始，还可以在激活 SNMP 时启用 SNMP 的写保护访问。团体字符串的含义和属性 SNMP 社区字符串（也称为社区名称）类似于 ID 或密码，用于访问设备（例如路由器）的信息/统计信息。为了提高访问的安全性，请更改 CPU 属性中的默认社区字符串。SNMP 管理器在收到 SNMP 代理发出的验证请求时通过传输团体字符串来验证自己的身份。团体字符串作为纯文本传输。SNMP 只读操作 (GET) 的默认团体字符串是“public”。SNMP 读写操作 (SET) 的默认团体字符串是“private”。团体字符串的字符数：1-240。团体字符串支持以下字符：a-z A-Z 0-9 - . 在用户程序中激活/取消激活 SNMP 除了 CPU 属性中的组态，还可在用户程序中激活或禁用 SNMP。为此，将数据记录 0xB071 传送到 CPU 的 PROFINET 接口。在该记录中，包含 SNMP 是否激活/取消激活的代码。无论将数据记录传送到哪个 PROFINET 接口，数据记录都适用于 CPU 的所有接口。传送 0xB071 数据记录的一种方法：在数据块中定义数据集结构，并在程序循环 OB（例如 OB1）中通过指令“WRREC”（写入数据记录）向 CPU 的 PROFINET 接口传送数据。为此，请执行以下操作步骤：1. 在 STEP 7 中，创建一个包含数据记录 0xB071 结构的数据块。下表列出了数据记录 0xB071 的结构：字节 元素 代码 说明 0 到 1 BlockID 0xF003 例如，在程序循环 OB (OB1) 中通过“WRREC”指令（写入数据记录）将数据记录 0xB071 传送到 CPU 中。将 CPU 中集成的 PROFINET 接口作为硬件 ID。SNMP 组态和用户程序的相互作用 SNMP 设置通过用户程序“激活/禁用”不会 yongjiu 存储在 CPU 中。例如，每次电源关闭/电源接通转换、下载新硬件配置或复位为出厂设置后，组态的设置会再次生效。从 CPU 下载组态（“上传设备作为新站”）时，将采用组态的 SNMP 设置（已激活/已取消激活）。先前由用户程序中的数据记录设置的 SNMP 设置将被忽略。团体字符串只能在组态中更改；团体字符串不能通过用户程序中的数据记录来设置。但是，可以通过数据记录激活组态的团体字符串。例如：已在 S7-1500 CPU 的组态中将 SNMP 设置为取消激活。更改 CPU 属性中的默认团体字符串，然后将组态下载到 CPU 中。然后，通过数据记录传输激活 SNMP。结果：将采用更改后的团体字符串。对于固件版本低于 V3.0 的 S7-1500 CPU，当激活 SNMP 时，预设的社区字符串（“public”和“private”）始终有效。

5.7.2 通过数据记录传送激活/取消激活

SNMP : CPU 1516-3 PN/DP 的示例简介要使用 SNMP 管理网络基础设施、CPU 和 IO 设备，请为 CPU 15163 PN/DP 激活 SNMP。以下示例显示了为此需要传送到 PROFINET 接口的 0xB071 数据记录。要求 CPU 15163 PN/DP 固件版本 V2.0 及更高版本 STEP 7 版本 V14 或更高版本解决方法将数据记录 0xB071 传送到 CPU 的 PROFINET 接口。因此，SNMP 在 CPU 的所有 PROFINET 接口中启用。以下示例说明如何在全局数据块中创建数据记录并在程序循环 OB (例如 OB1) 中将其传送到 PROFINET 接口 (Local~PROFINET\_interface\_1)。要在 CPU 15163 PN/DP 的已寻址 PROFINET 接口中激活 SNMP，请按以下步骤操作：1. 创建一个全局数据块。2. 指定一个名称，例如“ActivateSnmp”。使用 S7-1500R/H CPU 激活/取消激活通过 SNMP 进行数据记录传送在 S7-1500R/H 系统中，可像使用标准 CPU 一样在用户程序中激活/禁用 SNMP。但是，两个 CPU 的 PROFINET 接口 (X1、X2、...) 具有不同的硬件 ID。例如，左侧 CPU 的 PROFINET 接口 X1 与右侧 CPU 的 PROFINET 接口 X1 具有不同的硬件 ID。S7-1500R/H 系统不会自动同步两个 CPU 的 SNMP 状态 (激活/禁用)。通过“WRREC”指令设置的 SNMP 状态 (激活/禁用) 仅在 PROFINET 接口通过“WRREC”指令进行寻址的 CPU 中生效。示例：S71500R/H 系统处于“RUN Redundant”系统状态。例如，如果左侧 CPU 的 PROFINET 接口使用“WRREC”指令寻址，则左侧 CPU 的 SNMP 状态将发生变化。右侧 CPU 的 SNMP 状态保持不变。如果左侧 CPU 发生故障或被更换，则 SYNCUP 之后 SNMP 状态不发生变化。解决方法：调用“WRREC”指令 2 次。第一次调用“WRREC”指令时，寻址左侧 CPU 的 PROFINET 接口的硬件 ID。再次调用“WRREC”指令。此时，寻址右侧 CPU 的 PROFINET 接口的硬件 ID。PROFINET 接口 X1 的硬件 ID：左侧 CPU 的 PROFINET 接口 X1 的硬件 ID 为 65164 (默认名称：Local1~PROFINET-interface\_1)。右侧 CPU 的 PROFINET 接口 X1 的硬件 ID 为 65364 (默认名称：Local2~PROFINET-interface\_1)。通过 PROFINET 接口 X1 的相应硬件 ID 进行寻址的方法，也在以下示例中用于调用两个 R/H CPU 的“WRREC”指令。说明将数据记录传送到备用 CPU 只有在 S71500R/H 系统达到“Run REDUNDANT”系统状态后，才可将数据记录传送到备用 CPU 的已寻址 PROFINET 接口。否则，数据记录无法传送到备用 CPU 的寻址 PROFINET 接口。S71500R/H 系统达到系统状态“Run REDUNDANT”时，将启动 CPU 冗余错误 OB (OB72)。OB72 的“Fault\_ID”变量包含错误代码“B#16#03”或“B#16#06”。示例：两 R/H CPU 的 WRREC 调用要通过传送数据记录在两个 CPU 的已寻址 PROFINET 接口中激活/取消激活 SNMP，请按以下步骤操作：1. 创建一个全局数据块。2. 指定一个名称，例如“ActivateSnmp”。组织块“CPU 冗余错误”(OB72) 添加到用户程序中。相关 OB72 示例程序，请参见下一部分。5. 打开程序循环 OB (OB1)。6. 在 OB1 2 中，执行“WRREC”指令以将数据记录传送到两个 CPU 分别寻址的 PROFINET 接口。相关 OB1 示例程序，请参见下一部分。结果：0xB071 数据记录被分别传送到寻址的两个 CPU 的 PROFINET 接口。OB72 和 OB1 组织块的编程示例打开已添加的 OB72。使用以下程序代码，判断 R/H 系统是否已进入“Run REDUNDANT”状态，并设置“WRREC”指令的启动命令：//-----//

```

Check redundancy state and set "snmpWrite"//-----IF #Fault_ID = B#16#03
OR #Fault_ID = B#16#06 THEN"ActivateSnmp".snmpWrite := TRUE;END_IF;打开程序循环 OB
(OB1)。使用以下程序代码，可运行 2 条“WRREC”指令以将数据记录传送到两个 CPU 分别寻址的
PROFINET 接口：//-----// Start writing SNMP
settings//-----IF "ActivateSnmp".snmpWrite THENIF (NOT
"ActivateSnmp".plcLeft.snmpWrDone)AND (NOT "ActivateSnmp".plcLeft.snmpWrError) THEN使用 PG
进行通信时，CPU
或其它具备通信功能的模块可在工程师站进行数据交换 (例如，PG、PC)。可以通过 PROFIBUS 和
PROFINET 子网进行数据交换。此外，还支持 S7 子网之间的网关。PG 通信具有装载程序和组态数据、
运行测试以及评估诊断信息所需的功能。这些功能集成在具有通信功能的模块的操作系统中。说明自
TIA Portal 版本 V17 起，支持将 TLS (传输层安全) 协议用于编程设备/HMI
间通信，以确保采用标准化安全机制的编程设备/PC 与 CPU
之间数据交换的安全性。有关详细信息，请参见以下章节：安全通信要求 (页 62) PG/HMI 间安全通信
(页 87)要求 编程设备/PC 与具有通信功能的模块进行物理连接。如果需要通过 S7
路由来访问具有通信功能的模块，则必须在参与的站 (S7

```

路由器和端点)中装载硬件组态。在线连接步骤若要实现编程设备通信,必须建立与 CPU 的在线连接:1. 在 STEP 7 的项目树中选择 CPU。2. 选择“在线 > 转至在线”(Online > Go online) 菜单命令。3. 在“转至在线”(Go online)对话框中,针对在线连接进行以下设置: – 在“编程设备/PC 接口类型”(Type of PG/PC interface)下拉列表中,选择接口类型(如 PN/IE)。 – 在“PG/PC 接口”(PG/PC interface)下拉列表中,选择待建立在线连接的 PG/PC 接口(如,工业以太网卡)。 – 从“连接到接口/子网”(Connection to interface/subnet)下拉列表,选择用于将编程设备/PC 物理连接的接口或 S7 子网。 – 如果可以通过 S7 路由器(网关)访问具有通信功能的模块,请从“第一网关”(1st gateway) 下拉列表选择用于连接相关子网的 S7 路由器。