西门子工业触摸屏经销总代理商

产品名称	西门子工业触摸屏经销总代理商
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

西门子工业触摸屏经销总代理商使用 S7-1500R/H CPU 时，加载过程中仅将机密 PLC
组态数据的密码加载到其中一个 CPU中。为确保同步过程正常运行且伙伴 CPU
正常运行，同步前需通过“ 在线与诊断 ”(Onlineand Diagnostics) 编辑器将该密码传送到伙伴 CPU 中： –
在“ 在线和诊断 ”(Online and diagnostics) 视图中，可指定区域“ 保护机密 PLC
组态数据的密码 ”(Password to protect confidential PLC configuration data)。 –
输入所需密码，并单击“ 设置 ”(Set) 按钮。如果输入的密码正确，则伙伴 CPU 可使用受保护的 PLC
组态数据并启动同步过程。5.6.3.2 有关保护机密 PLC
组态数据的实用信息受安全标准保护的安全通信概念包括以下组成部分：
基于密码的密钥信息，用于保护机密组态数据（例如，证书、密码的私钥）。
保障参与者（例如，编程设备和 CPU）之间通信的标准化日志
(TLS)。“ 保护机密组态数据 ”原则下图简要显示了如何保护标准 S7-1500 CPU 等设备的机密组态数据：
首次下载时，两个组件项目和密钥信息将放在不同的存储区中。该项目位于装载存储器（存储卡）中，
密钥信息位于CPU 的存储区中。对于具有不同存储概念的其它目标系统（例如 S7-1200
CPU、软件控制器），实现方式取决于相应的存储概念，但存储原理相同。 ①
具有密码保护的机密组态数据的项目（此处：在装载存储器中，即存储卡中）②
使用受保护机密组态数据的密钥信息（通过密码生成）（此处：在 CPU 的存储区中）图 5-16 保护机密
组态数据的原理两个存储区可提高安全性涉及的组件像两个匹配的拼图一样彼此相关：项目绑定到下载
的密钥信息，下载的密钥信息绑定到组态期间分配的密码。项目和密钥信息必须匹配，否则 CPU
将无法启动

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起动器等两个独立存储区的原理也适用于不带存储卡的 S7-1200 CPU 和 S7-1500 CPU 版本，例如软件控制器或 PLCSim/PLCSim Advanced。在不带存储卡的版本中，使用两个单独的分区，以便可以独立管理两个信息项。图 5-17 两个独立存储区的原理5.6.3.3 更改密码具体操作步骤取决于是否已下载 CPU。如果 CPU 已下载，则包含密钥信息，可以通过该密钥信息使用受密码保护的 PLC 组态数据。更改密码 - 尚未下载组态只要尚未将组态下载到 CPU 中，就可以直接更改输入的密码或取消激活密码保护。要求 CPU 尚未下载。操作步骤1. 在网络视图或设备视图中打开 CPU 属性。2. 导航至区域“ 保护与安全 > 保护 PLC 组态数据 ”(Protection & Security > Protection of the PLCconfiguration data)。3. 单击“ 更改 ”(Change) 按钮或禁用选项“ 保护机密 PLC 组态数据 ”(Protect confidential PLCconfiguration data)。4. 在对话框中输入之前的有效密码。如果要更改密码，还需输入新密码并确认新密码。只要尚未将组态下载到 CPU 中，CPU 便处于配置阶段（参见“ 从下载到运行就绪的 CPU 行为(页 90) ”），可以使用组态的密码下载任何有效的组态。更改密码 - 组态已下载如果 CPU 已经下载组态，并且该组态受到机密 PLC 组态数据所用密码的保护，则必须首先将CPU 复位为出厂设置，并删除 CPU 中机密 PLC 组态数据的密码，或直接在线删除密码，然后进行设置。要求具有对 CPU 的写访问权限 CPU 必须处于 STOP 模式。操作步骤1. 在网络视图中选择 CPU。2. 在快捷菜单中，选择“ 在线和诊断 ”(Online & Diagnostics) 命令。如果还更改存储卡上的项目，即重新下载组态： – 在打开的在线和诊断视图中选择“ 复位为出厂设置 ”(Reset to factory settings) 区域。 – 激活选项“ 删除保护机密 PLC 组态数据的密码 ”(Delete password to protect confidentialPLC configuration data)。为了避免 CPU 重复启动，还需选择“ 格式化存储卡 ”(Formatmemory card) 选项。 – 然后使用更改后的组态和所需的密码下载项目。4. 如果无需更改存储卡上的项目，即仅设置密码： – 在“ 在线和诊断 ”(Online and diagnostics) 视图中，指定区域“ 保护机密 PLC 组态数据的密码 ”(Password for the protection of confidential PLC configuration data)。 – 单击“ 删除 ”(Delete) 按钮。如果“ 删除 ”(Delete) 按钮不可用，则表示尚未在 CPU 中设置密码。 – 输入所需密码，然后单击“ 设置 ”(Set) 按钮。如果输入了正确的密码，则 CPU 可以使用受保护的 PLC

组态数据。没有对 CPU 的写访问权限如果没有对装载存储器的写访问权限（读访问级别），请先从 CPU 上移除存储卡或从外部（例如在计算机中）删除存储卡，然后再使用选项“ 删除用于保护机密 PLC 组态数据的密码 ”(Delete password to protect confidential PLC configuration data) 复位为出厂设置。说明通过 CPU 模式选择开关复位为出厂设置通过模式选择开关恢复 CPU 的出厂设置时，还会删除 CPU 的 IP 地址，但不会删除用于保护机密 PLC 组态数据的密码。更多信息有关如何在采用备件的情况下继续操作的信息，请参见“ 更换部件方案的规则 (页 70) ”部分。5.6.3.4 重置密码可以重置机密 PLC 组态数据的保护。例如，若希望更改密码，但不再记得当前密码，则必须使用此操作。密码丢失 - 尚未下载组态首次通过 TIA Portal 下载 CPU 时必须输入密码，否则无法使用该 CPU 的 CPU 组态。要在 CPU属性中更改密码，还必须输入先前有效的密码。如果忘记密码，请执行以下操作：要求 CPU 尚未下载。

如果还更改存储卡上的项目，即重新下载组态： – 在打开的在线和诊断视图中选择“ 复位为出厂设置 ”(Reset to factory settings) 区域。 – 激活选项“ 删除保护机密 PLC 组态数据的密码 ”(Delete password to protect confidentialPLC configuration data)。为了避免 CPU 重复启动，还需选择“ 格式化存储卡 ”(Formatmemory card) 选项。 – 然后使用更改后的组态和所需的密码下载项目。4. 如果无需更改存储卡上的项目，即仅设置密码： – 在“ 在线和诊断 ”(Online and diagnostics) 视图中，指定区域“ 保护机密 PLC 组态数据的密码 ”(Password for the protection of confidential PLC configuration data)。 – 单击“ 删除 ”(Delete) 按钮。如果“ 删除 ”(Delete) 按钮不可用，则表示尚未在 CPU 中设置密码。 – 输入所需密码，然后单击“ 设置 ”(Set) 按钮。如果输入了正确的密码，则 CPU 可以使用受保护的 PLC 组态数据。没有对 CPU 的写访问权限如果没有对装载存储器的写访问权限（读访问级别），请先从 CPU 上移除存储卡或从外部（例如在计算机中）删除存储卡，然后再使用选项“ 删除用于保护机密 PLC 组态数据的密码 ”(Delete password to protect confidential PLC configuration data) 复位为出厂设置。说明通过 CPU 模式选择开关复位为出厂设置通过模式选择开关恢复 CPU 的出厂设置时，还会删除 CPU 的 IP 地址，但不会删除用于保护机密 PLC 组态数据的密码。更多信息有关如何在采用备件的情况下继续操作的信息，请参见“ 更换部件方案的规则 (页 70) ”部分。5.6.3.4 重置密码可以重置机密 PLC 组态数据的保护。例如，若希望更改密码，但不再记得当前密码，则必须使用此操作。密码丢失 - 尚未下载组态首次通过 TIA Portal 下载 CPU 时必须输入密码，否则无法使用该 CPU 的 CPU 组态。要在 CPU属性中更改密码，还必须输入先前有效的密码。如果忘记密码，请执行以下操作：要求 CPU 尚未下载。操作步骤1. 在网络视图或设备视图中打开 CPU 属性。2. 导航至区域“ 保护与安全 > 保护 PLC 组态数据 ”(Protection & Security > Protection of the PLCconfiguration data)。3. 单击“ 复位 ”(Reset)。请注意，CPU 的证书（例如 Web 服务器、OPC UA 服务器、PG/PC 通信和 HMI 通信的证书）在复位后无法再继续使用，必须重新创建和分配。 – 如果证书管理器中使用全局安全设置，则必须通过证书管理器重新分配证书。 – 如果证书管理器中未使用全局安全设置，则必须重新创建和分配证书。4. 确认重置密码。保护机密 PLC 组态数据的选项仍处于激活状态。删除密码 – 组态已下载如果 CPU 已经下载组态，并且该组态受到机密 PLC 组态数据所用密码的保护，则为了下载新项目，请在线删除机密 PLC 组态数据的密码，然后指定新密码。要求 具有对 CPU 的写访问权限 CPU 必须处于 STOP 模式。操作步骤1. 在网络视图中选择 CPU。2. 在快捷菜单中，选择“ 在线和诊断 ”(Online & Diagnostics) 命令。3. 在区域“ 保护机密 PLC 组态数据的密码 ”(Password to protect confidential PLC configurationdata) 中，单击“ 删除 ”(delete) 按钮。如果“ 删除 ”(Delete) 按钮不可用，则表示尚未在 CPU 中设置密码。注意删除机密组态数据的密码如果删除密码，而下载的项目需要相应的密码，则该项目在没有密码的情况下无法继续工作。4. 如需要，可通过“ 设置 ”(Set) 按钮输入新密码。5. 重启 CPU。更多信息有关更改密码的信息，请参见“ 更改密码 (页 65) ”部分。通过 SIMATIC 存储卡分配密码如果要在不使用 TIA Portal 的情况下将用于保护机密 PLC 组态数据的密码传送到 CPU，可以使用 SIMATIC 存储卡来实现此功能。SIMATIC 存储卡适用于以下用途： 准备一个新的 CPU如果再次设置 CPU，则组态时应设置用于保护机密 PLC 组态数据的密码。完成此组态后，可以使用包含所需项目的另一个 SIMATIC 存储卡。（S7-1200 CPU：具有传送作业的“ 传送 ”卡也可用于在 CPU 上安装程序）。 CPU 具有用于保护机密 PLC 组态数据的密码，但该密码与项目不匹配如果密码不相同，则可使用 CPU

中的存储卡设置正确的密码。（S7-1200 CPU：配有 SIMATIC“ 传送 ”卡或 SIMATIC“ 程序 ”卡）。 在 CPU 中重置用于保护机密 PLC 组态数据的密码准备处置旧 CPU 或为 CPU 准备新项目。要求 TIA Portal 版本 V17 及以上版本基本操作步骤1. 创建具有“ 设置密码 ”作业的 SIMATIC 存储卡该操作按照特殊模式创建文件夹和文件结构，并将用于保护机密 PLC 组态数据的密码以纯文本形式写入到 SIMATIC 存储卡的特殊文件中。参见以下描述。2. 将准备好的 SIMATIC 存储卡插入 CPU 中并接通 CPU 电源。PLC 读取密码并对其进行处理，然后将结果存储在内部存储器中。任何现有数据都将被覆盖。3. 移除 SIMATIC 存储卡并重启 CPU。结果 (S7-1500)：CPU 读取 SIMATIC 存储卡时，LED 指示灯的闪烁方式与固件更新时相同。CPU 设置密码时，RUN/STOP LED 指示灯闪烁。该过程成功完成后，RUN/STOP LED 指示灯呈黄色亮起且 MAINT LED 指示灯呈黄色闪烁。操作结果以成功或错误消息的形式显示在诊断缓冲区中。如果无法设置密码，则错误 LED 指示灯将与其它 LED 指示灯一起闪烁。创建具有“ 设置密码 ”作业的 SIMATIC 存储卡1. 在根目录中创建一个名为“ SET_PWD.S7S ”的文件夹。2. 在该文件夹中创建一个名为“ PWD.TXT ”的文本文件，其中仅包含文本形式的密码3. 在存储卡的根目录中创建一个名为“ S7_JOB.S7S ”的文本文件，其中包含内容“ SET_PWD ”。此文件作为“ 作业文件 ”，用于分配保护 PLC 的机密 PLC 组态数据的密码。4. SIMATIC 存储卡上的文件结构显示如下：说明SIMATIC 存储卡的安全存储将 SIMATIC 存储卡存储在只有授权人员才能访问的安全位置。规则和建议 设置密码必须在安全的环境中进行。文本文件“ PWD.TXT ”的内容定义用于保护机密 PLC 组态数据的密码。该密码必须与 CPU 组态中分配的密码匹配。 要重置 PLC 的现有密码，文本文件“ PWD.TXT ”必须为空，即文件大小为 0 字节。 使用任意文本编辑器来创建文本文件。推荐的文本格式为“ UTF-8 ”。文件夹名称和文件名不区分大小写。但是，密码本身区分大小写。 不要在末尾处输入 CR/LF 字符（PWD.TXT 或 S7_JOB.S7S）。5.6.3.6 备份和恢复 CPU 时的特殊功能在 TIA Portal 中，可备份 CPU 的功能组态以便后期访问。即，之后可恢复最初备份的状态。备份后用户便可以下载修改后的组态，例如，测试产品增强功能，更改程序以在系统中进行故障排除，或者可以在测试的基础上更换组件。然后，可恢复该 CPU 最初备份的组态。备份组态。在备份 CPU（TIA Portal 中的“ 在线 ”(Online) 菜单，“ 从在线设备下载备份 ”(Load backup fromonline device)）时，也会备份用于保护机密 PLC 组态数据的密码。恢复备份恢复 CPU 的备份时（TIA Portal 中的菜单“ 在线 ”(Online)，对标记的备份执行命令“ 下载到设备 ”(Download to device)），只有满足以下条件，CPU 才能与 PG/PC 或 HMI 进行通信： 恢复保护机密 PLC 组态数据时使用密码保护的组态后，该 CPU 中必需包含此密码。否则，CPU 无法访问该组态数据，因此无法启动。补救措施如果发生上述错误（即保护机密 PLC 组态数据的密码与备份不匹配），则必须删除保护 CPU中机密 PLC 组态数据的密码，然后设置正确的密码。重新启动 CPU 后，备份功能恢复正常。有关避免错误和错误处理的提示以下说明列出了一些可能导致 CPU 错误消息的用例。诊断缓冲区提供信息用于保护机密组态数据的密码与下载的组态不匹配时，CPU 会检测到该问题。诊断缓冲区中的消息指示可能的原因和补救措施，通常可以作为问题的解决方案。典型的“ 陷阱 ”为了避免或纠正错误，请注意以下情况：组态已下载？无论是否使用密码保护机密组态数据：如果没有下载的组态，CPU 便不会退出配置阶段。正在尝试下载包含组态密码的 CU，而 CPU 已经收到另一个密码。例如：CPU 已更换为库存中的另一个 CPU。更换的 CPU 件并未完全复位（通过选项“ 删除用于保护机密 PLC 组态数据的密码 ”(Delete password for protection of confidential PLCconfiguration data) 复位为出厂设置）。补救措施： – 准备更换 CPU 时，始终使用适当的设置（密码已删除）。 – 对于要下载的组态，使用已下载的组态中所使用的密码。 – 也可能下载了错误的项目/CPU 组态。检查正确的 CPU 组态是否可用。 – 使用在线功能“ 设置用于保护机密 PLC 组态数据的密码 ”(Set password to protectconfidential PLC configuration data) 删除密码或设置为与 CPU 组态相同的密码。然后重启设备。 如果 CPU 组态不使用密码，而已下载的组态需要用户自定义密码，则仍会发生错误。补救措施： – 使用在线功能“ 设置用于保护机密 PLC 组态数据的密码 ”(Set password to protectconfidential PLC configuration data) 删除密码或设置为与 CPU 组态相同的密码。然后重启设备。5.6.3.8 更换部件方案的规则分配用于保护机密 PLC 组态数据的密码也会对更换部件方案产生影响。更换部件方

案的规则请遵守以下更换部件方案的规则：通过 TIA Portal 组态更换的 CPU 更换 CPU
不应具有组态或用于保护机密 PLC
组态数据的密码。优势：无论是否组态了密码，都可以将项目下载到更换 CPU
中，而无需进行任何其它准备工作。 如果已组态更换 CPU，则必须将 CPU
复位为出厂设置，同时设置以下选项： – “ 删除保护机密 PLC 组态数据的密码 ”(Delete password for protection of confidential PLCconfiguration data)