西门子工业电线电缆经销总代理商

产品名称	西门子工业电线电缆经销总代理商
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

西门子工业电线电缆经销总代理商 将 TMAIL_C 指令的 MAIL_ADDR_PARAM 参数与 TMAIL_V4_SEC 数据类型的变量进行互连。在以下示例中，TMAIL_C 指令的 MAIL_ADDR_PARAM 参数已与“ MailConnectionSEC ”变量（TMAIL_V4_SEC 数据类型）进行互连。图 5-33 TMAIL_C 指令通过通信模块接口与邮件服务器建立安全连接要通过一个通信模块与邮件服务器建立安全通信，则需手动创建一个系统类型为TMAIL_V4_SEC、TMAIL_QDN_SEC 或 TMAIL_V6_SEC 的数据块，分配参数并在 TMAIL_C 指令中直接调用该数据块。要求： TMAIL_C 指令，版本 V4.0 S7-1500 CPU 固件版本 V2.0 及以上版本，通信模块 CP 15431 固件版本 V2.0 及以上版本 ET 200SP CPU 固件版本 V2.0 及以上版本，通信模块 CP 1542SP1 (IRC) 固件版本 V1.0 及以上版本 已将邮件服务器的所有 CA 证书分配给 CP（TLS 客户端），而且已将组态下载到 CPU 中。 在 CPU 中，设置当前的日期和时间。有关如何通过通信模块的接口与邮件服务器建立安全连接的信息，请参见 STEP 7 在线帮助。PG/HMI 间安全通信5.6.5.1 基于标准化安全机制的 PG/HMI 通信在 V17 及以上版本中集成有最新型控制器和最新型 HMI 设备，TIA Portal、STEP 7 和 WinCC的主要组件可实现创新型 PG/PC 和 HMI 标准安全通信（简称为 PG/HMI 通信）。具体涉及以下 CPU 系列： S7-1500 控制器系列固件版本 V2.9 及以上版本 S7-1200 控制器系列固件版本 V4.5 及以上版本 软件控制器固件版本 V21.9 及以上版本 SIMATIC 启动控制器固件版本 V2.9 及以上版本 PLCSim 和 PLCSim Advanced 版本 V4.0HMI 组件经更新以支持 PG/HMI 间安全通信： 使用 WinCC 精简版、精智版和gaoji版组态的面板或 PC 安装有 WinCC 专业版运行系统 的 PC WinCC Unified PC 和精智面板还更新了 V6.1 及以上版本的 SINAMICS RT SW 和 V17 及以上版本的 STARTDRIVE。PG/HMI 通信的特性PG 通信和 HMI 通信最显著的一个特点是简单：在安装 TIA Portal 的编程设备和 CPU 之间建立在线连接（例如，以下载程序）只需几步简单的操作。此在线连接基于公认的 SIMATIC 通信标准，可满足机密性和完整性等方面的要求。在将机器和系统集成到开放 IT 环境过程中，必须确保编程设备/HMI 设备与 CPU 之间的通信不仅要有效保护敏感数据的完整性和机密性，同时还要确保其符合公认的安全标准，从而能够应对未来的挑战。在 TIA Portal 版本 V14 中，基于用户程序的“ 开放式用户通信 ”过程已扩展为“ 安全的开放式用户通信 ”机制。同时还建立了其它基于证书的通信机制（HTTPS、Secure SMTP over TLS 或 OPCUA）。在 TIA Portal 版本 V17 即以上版本中，还对 PG/HMI 通信进行了升级：在此，TLS（传输层安全）协议用于采用标准化安全机制的 PG/HMI 间安全通信。更改的内容用于提高安全性的附加可选密码上述设备的组态形式中最显著的变化是能够分配密码以保护相

应 CPU 的敏感组态数据。敏感组态数据包括诸如私钥等数据，基于证书的协议正常运行（安全通信）需要私钥，对于 TIAPortal V17 及以上版本，PG/HMI 通信也需要私钥。在 TIA Portal 中输入密码时，可以使用策略设置来检查已分配的密码。这样，可确保企业遵循既定的密码策略。如果计算机或系统已采用其它类似保护，而无需实施基于西门子工业深度防御机制的保护措施，则无需进行密码分配。如果已采取相应措施保护 TIA Portal 项目和 CPU 组态防止未经授权的访问，则可以不使用密码。警告如果不使用密码，则私钥仅获得弱保护请注意，如果未使用密码来保护受信任的组态数据

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

PG/HMI 与 CPU 之间基于证书的通信由于 PG/HMI
通信基于证书，因此调试过程中要求接受服务器证书。通过其它参数分配选项，可以确定 CPU
运行期间的行为：例如，可以指定 CPU 允许连接到不支持 PG/HMI
间安全通信的设备。维护/更换部件方案为了在更换部件方案中更换 CPU
时不发生故障，必须遵守特定的规则（参见“ 更换部件方案的规则 (页
70) ”）。更多信息有关如何保护机密组态数据的概览，请参见“ 保护机密的组态数据 (页
62) ”部分。5.6.5.2 PG/HMI 间安全通信的其它设置除了分配用于保护机密 PLC

组态数据的密码外，还提供其它设置选项以确定 CPU 运行期间的行为。PG/PC 和 HMI 通信模式可以设置 CPU 与编程设备和 HMI 设备的通信方式： 仅通过 PG/HMI 间安全通信 通过 PG/HMI 间安全通信和先前使用的 PG/HMI 通信（简称为 “ 传统的 PG/HMI 通信 ”）。操作步骤1. 在 CPU 属性中，导航至区域 “ 保护与安全 > 连接机制 ” (Protection & Security > Connectionmechanisms)。2. 选择要使用的选项。选择证书或生成新证书如果选择用于 PG/HMI 通信的连接机制，则可以选择符合条件的 PLC 通信证书来保护连接，或者由 TIA Portal 生成证书。如果已分配密码或已取消激活保护机密 PLC 组态数据的选项（即未设置密码），则 “ 保护与安全 > 连接机制 ” (Protection & Security > Connection mechanisms) 中已预先设置了具有适当设置和有效默认名称的证书。操作步骤如果要通过 TIA Portal 生成新证书，或者要选择其它现有证书：1. 在 “ PLC 通信证书 ” (PLC communication certificate) 字段中，单击三个点以展开该字段。2. 选择所需证书，或单击 “ 添加 ” (Add) 按钮。3. 添加证书时，将显示一个包含证书设置选项的对话框。用于设置 “ TLS 服务器 ”，可以更改其它参数（例如名称、哈希算法）。应用证书管理的通用规则。例如，如果要生成 CA 证书，则必须选择 “ 证书管理器的全局设置 ” (Global settings for the certificate manager) 选项。此外，也可选择生成自签名 PLC 证书有关证书管理主题的说明，请参见 “ 使用 TIA Portal 进行证书管理 (页 53) ” 部分。5.6.5.3 PG 与 CPU 之间基于证书的通信的提示基于证书的 PG/PC 通信（PG/PC 间安全通信）意味着 CPU 的通信伙伴（安装了 TIA Portal 的编程设备）必须信任 CPU 的设备证书，才能下载连接。简而言之，从 TIA Portal 的角度来说，可使用以下方式信任 CPU 的证书： 安装了 TIA Portal 的编程设备已具有 CPU 的设备证书，例如，已在项目中创建或导入证书。此时，将系统自动运行证书检查，而无任何提示。 安装了 TIA Portal 的编程设备不具有 CPU 的设备证书，例如，CPU 通过 “ 可访问站 ” (Accessible stations) 确定，而在项目中不可用。此时，TIA Portal 将询问 TIA Portal 用户该证书是否可信。只有通过大量的工作才能做出判断，因为 CPU 不在眼前，因此无法立即鉴定真伪。 安装了 TIA Portal 的编程设备具有 CA 证书（证书颁发机构），并且 TIA Portal 可通过网络访问的所有 CPU 都具有该 CA 证书颁发的设备证书。该解决方案的优势：即使通信伙伴的设备证书在 TIA Portal 中不可用，TIA Portal 仍可以自动检查设备证书。下文将详细介绍 CA 证书（证书颁发机构）解决方案。要求可以使用 TIA Portal 的证书颁发机构创建 CPU 的设备证书，并使用现有 CA 证书为设备证书签名。还可以在 TIA Portal 中导入并使用另一个证书颁发机构。必须启用证书管理器的全局安全策略。只有完成此设置，才能生成 CA 签名的证书。另请参见 “ 使用 TIA Portal 进行证书管理 (页 53) ” 导出编程设备的 CA 证书要在创建和分配证书后导出相应的 CA 证书，请按照以下步骤进行操作：1. 打开项目树中全局安全设置下的证书管理器。2. 针对要导出的证书，选择 “ CA 证书 ” (CA certificates) 表。3. 单击右键，打开所选证书的快捷菜单。4. 单击 “ 导出 ” (Export)。5. 选择证书的导出格式和存储位储 CA 证书为确保安装了 TIA Portal 的编程设备能够识别导出的证书从而启用自动证书检查，请按照以下步骤进行操作：1. 将上一步骤中导出的 CA 证书复制到以下目录：C:\ProgramData\Siemens\Automation\Certstore\Trusted2. 启动 TIA Portal。在巡视窗口的 “ 信息 ” (Info) 选项卡中，每个 CA 证书对应显示一条消息，说明该 CA 证书是否可以成功传输到 TIA Portal 的 CA 存储区。如果出错，并不输出详细原因。向 TIA Portal 证书吊销列表 (CRL) 添加设备证书如果出现关联的密钥不再安全等情况，可以选择将设备证书单独添加到证书吊销列表 (CRL)。当 TIA Portal 与设备证书位于证书吊销列表中的 CPU 建立连接时，TIA Portal 中将出现一个对话框，询问是否仍要信任该证书。如果拒绝，将无法建立连接。要向证书吊销列表中添加设备证书，请按照以下步骤操作：1. 将设备证书复制到以下目录：C:\ProgramData\Siemens\Automation\Certstore\CRL2. 启动 TIA Portal。在巡视窗口的 “ 信息 ” (Info) 选项卡中，每个证书对应显示一条消息，说明该证书是否可以成功传输到 TIA Portal 的 CRL 存储区。如果出错，并不输出详细原因。5.6.5.4 从下载到运行就绪的 CPU 行为为确保 CPU 与编程设备或 HMI 设备之间的通信安全，必须首先具有证书。用于生产运行的证书仅在项目下载到 CPU 之后发布。为了保障初始下载过程的安全，CPU 首先创建一个自签名证书。下文中介绍了建立连接的不同阶段。关于初始建立连接并进而下载到 CPU 的要求 CPU 中未设置保护机密 PLC 组态数据的密码。如果该 CPU 已设置并因此设置有一个保护机密 PLC 组态数据的密码，则该密码必需与待加载项目的密码相匹配。 具有 CPU 组态（包括机密 PLC

组态数据的密码）和用户程序的项目可供使用。 CPU 处于 STOP 模式。 编程设备和 CPU 直接互连并且位于受保护的环境中；即，可以识别要下载的 CPU，并控制CPU 与编程设备之间的连接。首次与 CPU 建立连接 - 配置阶段用于下载 CPU 而建立的第一个连接采用 PG/HMI 间安全通信并由 TLS 程序提供安全保障。但 CPU 可使用制造商的设备证书（如果有），或使用自签名的证书建立连接。在该阶段中，此 CPU 仅能有限范围内使用。在此阶段中，CPU 将等待基于密码的密钥信息。即，保护机密PLC 组态数据的密码。此阶段下称配置阶段。诊断缓冲区中的消息指示 CPU 处于配置阶段。调试期间可能存在的安全风险在调试过程中，CPU 提供制造商的设备证书（如果有）或自签名证书，必须信任该证书才能建立连接。仅当编程设备与 CPU 处于受保护网络、并彼此直接相连时，才会信任此证书。在不受保护的环境中，这些证书可能被操纵，允许攻击者访问编程设备/HMI 与 CPU 之间的通信（例如通过中间人攻击）。配置阶段结束TIA Portal 不会在项目中存储机密 PLC 组态数据的密码本身或通过密码生成的密钥信息。因此，首次下载项目或下载新项目时，会在对话框中请求输入密码，并将该密码作为密钥信息传送到 CPU。只有在执行此步骤之后，CPU 才能使用受保护的 PLC 组态数据 - 这样便可完成配置阶段，CPU 才能开始运行。如果未使用密码保护机密 PLC 组态数据，则首次下载 CPU 时无需输入密码。此时，对 PG/HMI数据通信无影响；但需注意，机密的 PLC 组态数据（如，私钥）几乎无任何保护，无法防止未经授权的访问。PG/HMI 通信启动当 CPU 已下载并收到用于 PG/HMI 间安全通信的 CPU 证书后，编程设备将再次连接 - 此时基于下载的 CA 证书。使用 HMI 安全通信在 TIA Portal V17 及以上版本中，如果 CPU 和 HMI 设备均满足 HMI 安全通信要求，则可使用这种通信方式。要使用 HMI 安全通信，HMI 设备可在建立通信连接时通过 CPU 发送的 PLC 通信证书对该 CPU进行身份验证，确定该 CPU “ 可信 ”。仅当满足以上条件时，才能进行 HMI 安全通信。在本章节中，将介绍各 HMI 设备将 PLC 通信证书手动标记为 “ 可信 ” 的具体措施。要求 CPU 和 HMI 设备支持 HMI 安全通信。当前项目位于 CPU 中（TIA Portal V17 及更高版本）。组态 HMI 安全通信1. 组态 HMI 设备的报警视图。说明如果报警视图缺失，则无法设备连接错误。2. 组态 CPU 中所需的安全设置。选择 PLC 通信证书，保护 HMI 连接安全；或通过 TIA Portal生成一个 PLC 通信证书。3. 组态 CPU 与 HMI 设备间的 HMI 连接。4. 将项目下载到 CPU 和 HMI 设备中。在项目传送过程中，系统将 PLC 通信证书传送到 CPU和 HMI 设备中。必要时，还将传输 CA（证书颁发机构）证书。将 PLC 通信证书设置为可信连接建立时，CPU 将该 PLC 通信证书传送到 HMI 设备中。 如果该 PLC 通信证书在 HMI 设备中的状态已标记为 “ 可信 ”，则 CPU 与 HMI 设备间将自动建立一条 HMI 安全通信。 如果该 PLC 通信证书在 HMI 设备中的未标记为 “ 可信 ”，则在 HMI 设备的报警视图中将显示一条消息指示该 CPU 不可信，并提供一个错误代码。此时，需在 HMI 设备上将该 PLC 通信证书标记为 “ 可信 ”。根据 HMI 设备类型，执行以下操作步骤。第二代精简面板1. 在 Start Center 中，选择 “ Settings > Internet Settings > Certificate store ”。2. 在 “ Available certificates in Device ” 列表中，选择该 CPU 的 PLC 通信证书。3. 按下 “ Trust ”。