

西门子工业以太网电缆经销总代理商

产品名称	西门子工业以太网电缆经销总代理商
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

西门子工业以太网电缆经销总代理商说明ServerCapabilities S7-1500 CPU 的 OPC UA 服务器不支持该变量。SupportedPrivateKeyFormats 此变量用于指定允许使用的私钥格式。对于 S7-1500 CPU，仅允许使用“PEM”（字符串数组）MaxTrustListSize 此变量用于指定信任列表的最大大小。MulticastDnsEnabled 此变量用于指定是否支持组播 DNS。对于 S7-1500 CPU，该值为“False”。CertificateGroups 该对象（文件夹）用于组织 OPC UA 服务器所支持的所有证书组。这些证书组包含运行期间可动态更新的对象。例如，每个证书组包含一个信任列表，还包含一个或多个分配给服务（例如 OPC UA 应用程序）的证书。有关 CertificateGroups 对象的结构以及此对象中提供的方法和属性的详细信息，请参见下一节。CreateSigningRequest 该方法具有以下参数：参数数据类型 说明[in] certificateGroupId NodeId CertificateGroup 对象的 NodeId。 [in] certificateTypeId NodeId 请求的证书类型。允许使用的证书类型列表由证书组的“CertificateTypes”变量指定。例如，OPC UA 服务器使用的证书类型是“RsaSha256ApplicationCertificateType”，Web服务器使用的证书类型是“HttpsCertificateType” [in] subjectName String 证书请求中请求的主题名称。如果未指定，则使用证书的当前主题名称。 [in] regeneratePrivateKey Boolean True：服务器生成新私钥。该密钥会一直保存到调用签名证书匹配的 UpdateCertificate 方法为止。False：服务器使用既有私钥。 [in] nonce ByteString 用于生成新私钥的额外随机数（参见regeneratePrivateKey）。长度必须至少为 32 字节。 [out] certificateRequest ByteString PKCS #10 - DER 编码证书请求。方法结果代码结果代码 说明Bad_InvalidArgument certificateTypeId、certificateGroupId 或subjectName 无效。Bad_UserAccessDenied 当前用户不具备所需的功能权限

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

通过 CreateSigningRequest 生成证书。未提供私钥。新私钥和新证书在服务器之外生成。两者均通过 UpdateCertificate 进行更新。证书通过现有证书的私钥生成并签名。未提供私钥。参数 数据类型 说明[in] certificateGroupId NodeId CertificateGroup 对象的 NodeId。 [in] certificateTypeId NodeId 请求的证书类型。允许使用的证书类型列表由证书组的 “ CertificateTypes ” 变量指定。 [in] certificate ByteString 替换现有证书的 DER 编码证书。 [in] issuerCertificates ByteString 颁发机构证书[in] privateKeyFormat String 私钥格式。目前仅支持 PEM。如果未指定privateKey：零或空字符串。 [in] privateKey ByteString 按 privateKeyFormat 中指定的格式进行编码的私钥。 [out] applyChangesRequired Boolean 指示使用新证书前必须调用 “ ApplyChanges ” 方法。方法结果代码结果代码 说明Bad_InvalidArgument certificateTypeId 或 certificateGroupId 无效。 Bad_CertificateInvalid 证书无效或格式不受支持。 Bad_NotSupported 私钥无效或格式不受支持。 Bad_UserAccessDenied 当前用户不具备所需的功能权限。 Bad_SecurityChecksFailed 验证证书完整性时出错。应用更改该方法没有参数。方法结果代码结果代码 说明Bad_UserAccessDenied 当前用户不具备所需的功能权限该方法具有以下参数：参数 数据类型 说明[out] certificates ByteStrings 被拒绝的 DER 编码证书列表。由于不会存储被拒绝的证书，此方法目前返回一个空列表（空数组）。方法结果代码结果代码 说明Bad_UserAccessDenied 当前用户不具备所需的功能权限。 11.2.7.6 地址模型中的 CertificateGroups运行过程中，CPU（OPC UA 服务器）中可更新服务或应用程序的证书和信任列表位于地址模型中的 “ CertificateGroups ” 对象中，该对象是 S71500 CPU 中所有服务都有的一个证书组。对于 OPC UA 服务器证书，证书组的名称为 “ OPC UA server ”。地址模型中的 CertificateGroup下图显示了 “ ServerConfiguration ” 节点下方 “ CertificateGroups ” 对象的结构。在 STEP 7 (TIA Portal) 中，可更改 CertificateGroups 的 Display Name（例如，“ OPC UAserver ” 的显示名称）：1. 在巡视窗口（CPU 属性）中，导航至 “ 保护与安全 > 证书管理 ” (Protection & Security >Certificate management) 区域。2. 启用 “ 运行期间使用证书管理提供的证书 ” (Use certificates provided by certificatemanagement during runtime) 选项。3. 更改下表中证书组的组名称 (DisplayName)。允许 7 位 ASCII

格式的 1-64 字符。第一列包含已激活的可在运行时传送证书的服务，“ID”列包含用于在 CPU 内部引用证书的固定数字标识符。ificateTypes”节点“CertificateTypes”变量指定分配给服务器应用程序的证书类型的 NodeId。例如，OPC UA 服务器服务支持“RsaSha256ApplicationCertificateType”CertificateType，Web 服务器支持“HttpsCertificateTypeCertificateType”。“TrustList”节点信任列表对象的节点（TrustList 文件）定义了 OPC UA 文件类型（二进制编码流），其中包含有关证书和 CRL 的信息。此信息可在存储卡的“pki store\trusted\issuer”目录中读取和更新。该节点提供用于读取和更新的方法和属性。节点是 OPC UA 数据类型“TrustListDataType”的实例，其结构如下：参数 数据类型 说明 specifiedLists TrustListsMasks 该位掩码用于显示包含信息的列表。trustedCertificates ByteStrings 可信任的应用程序证书和 CA 证书列表 rustList”节点的方法和属性下方是“TrustList”下的各节点的描述，此等节点是对 Object Type “FileType”方法的补充。TrustList Type 由 FileType 派生而来（参见 OPC 100005：OPC 统一架构，第 5 部分：信息模型）。方法/属性（变量）说明 LastUpdateTime 此变量用于显示上次更新时间。OpenWithMasks 此方法允许客户端仅读取部分 TrustList。CloseAndUpdate 此方法用于关闭 TrustList 文件并应用更改。AddCertificate 此方法用于将单个证书添加到 TrustList。RemoveCertificate 此方法用于从 TrustList 中移除单个证书。方法说明 OPC UA 规范第 12 部分“发现和全局服务”中介绍了上述方法及其结果代码、属性和 TrustList 对象类型将 S7-1500 用作 OPC UA 服务器 11.3.1 关于 S7-1500 CPU 的 OPC UA 服务器的有效信息 11.3.1.1 S7-1500 CPU 的 OPC UA 服务器固件版本 V2.0 及以上版本的 S71500 CPU 均可作为 OPC UA 服务器。除了标准 S7-1500CPU，此特性同样适用于 S7-1500F、S7-1500T、S7-1500C、S7-1500pro CPU、ET 200SPCPU、SIMATIC S7-1500 软件控制器和 PLC SIM Advanced。约定：“S71500 CPU”同样包括上述的 CPU 类型。S7-1500 CPU OPC UA 服务器的基本知识 S7-1500 CPU 上所有集成的以太网接口，均可用于访问该 CPU 的 OPC UA 服务器。在以下条件中，不能借助 CP 通过自动化系统的背板总线直接访问 CPU 的 OPC UA 服务器：通过 TIA Portal V16 或更高版本进行组态 S7-1500 CPU 固件版本 2.8 或更高版本以及 CP 1543-1 固件版本 V2.2 或更高版本有关组态的信息，请参见“访问 OPC UA 应用程序 (页 144)”。不能借助 CM 通过自动化系统的背板总线直接访问 CPU 的 OPC UA 服务器。通过客户端进行访问时，服务器将以节点形式保存启用的 PLC 变量和其它信息（请参见“访问 OPC UA 服务器数据 (页 186)”）。这些节点相互连接并形成网络。OPC UA 将定义该网络的接入点（已知节点），可导航到下级节点。通过 OPC UA 客户端，可以读取、监视或写入 PLC 程序中的变量值，并调用服务器中可用的方法。在固件版本 V2.5 及以上版本中，可实现这些方法。具体信息，请参见关于服务器方法的有用信息 (页 243)。节点类别 OPC UA 服务器将基于节点提供相应的信息。节点可以是一个对象、变量、方法或属性。图 11-8 S7-1500 CPU 的 OPC UA 服务器地址空间示例在上图中，已选择“MyValue”变量（以灰色突出显示）。此变量位于节点类别为“Object”的“Memory”节点下。“Memory”位于“PLC_1”节点下（也是一个 Object）。地址空间节点通过引用进行连接（如，引用“HasComponent”）。即，节点与子节点之间为层级关系。通过引用，这些节点将构成一个网络。该网络可以为树形结构等。因此，节点网络也可称为地址空间。可从根节点开始，访问地址空间中的所有节 OPC UA 服务器的端点在 OPC UA 服务器的端点，将定义连接的安全级别。基于所用或期望的安全级别，在端点处需执行相应的连接设置。不同的安全设置建立安全连接之前，OPC UA 客户端会询问服务器采用哪些安全设置进行连接。服务器将返回服务器提供的所有安全设置（端点）的列表。端点结构端点由以下几部分组成：OPC 的标识符：“opc.tcp” IP 地址：192.168.178.151（在本示例中）OPC UA 的端口号：4840（标准端口）端口号可组态。消息的安全设置（消息安全模式）：“无”（None）、“签名”（Sign）、SignAndEncrypt。加密和 HASH 程序（Security Policy）：无，Basic128Rsa15、Basic256、Basic256Sha256（在本示例中）。下图显示了 OPC Foundation 的“UA Sample Client”。客户端已与 S7-1500 CPU 中 OPC UA 服务器的端点“opc.tcp://192.168.178.151:4840 -[SignAndEncrypt: Basic256Sha256: Binary]”建立了安全连接：该端点的安全设置为“SignAndEncrypt: Basic256Sha256”。说明选择安全策略尽可能严格的端点根据具体应用，为端点选择相应的安全策略，并在 OPC UA 服务器上禁用较不严格的安全策略。S7-1500 CPU OPC UA 服务器为确保端点最为安全（Basic256Sha256），要求具有 Sha256 证书。图 11-9 OPC 基金会的“UA Sample Client”程序仅当 OPC UA

客户端符合服务器端点的安全策略时，才能与服务器端点建立连接。OPC UA 服务器提供的信息 OPC UA 服务器可提供大量信息：客户端可能访问的 DB 元素以及 PLC 变量的值。这些 PLC 变量和 DB 元素的数据类型。有关 OPC UA 服务器和 CPU 的信息。因此，客户端可了解并读取相应的特定信息，无需具备之前的 PLC 程序和 CPU 数据。读取 PLC 变量时，无需询问 PLC 程序的研发人员。所有相关信息均存储在服务器中（如，PLC 变量的数据类型）。如果您熟知相关语法和 PLC 编程，则可直接访问 OPC UA 服务器，而无需先了解相关信息。

11.3.1.3 OPC UA 服务器运行期间的行为

运行过程中的 OPC UA 服务器激活服务器并将项目下载到 CPU 后，S7-1500 CPU 的 OPC UA 服务器会启动。此处介绍了如何激活 OPC UA 服务器。CPU STOP 操作状态的行为即使 CPU 切换到“STOP”模式，已激活的 OPC UA 服务器仍然保持运行状态。OPC UA 服务器会继续响应来自 OPC UA 客户端的请求。服务器响应的详细信息：如果用户请求 PLC 变量的值，则会获得 CPU 切换到或被设置为“STOP”模式之前的最新值。如果用户向 OPC UA 服务器写入值，则 OPC UA 服务器将接受这些值。但是，由于用户程序不是在“STOP”模式下执行的，所以 CPU 不会处理这些值。尽管如此，OPC UA 客户端仍可从 CPU 的 OPC UA 服务器读取 STOP 模式下所写入的值。在重新启动过程中，CPU 将在开始执行 PLC 变量时覆盖 STOP 模式下所写入的值。调用某个服务器方法时，系统将因为服务器方法（用户程序）当前未运行而输出错误消息 16#00AF_0000 (BadInvalidState)。操作模式转换 (STOP > RUN or RUN > STOP) 时，与 OPC UA 服务器的连接保持激活。例外：加载 OPC UA 相关数据，具体请参见下一章节。下载到 CPU 可能会影响 OPC UA 服务器如果在 OPC UA 服务器运行时加载 CPU，则可能需要根据加载的对象停止并重新启动服务器。在这种情况下，活动连接会中断，必须在服务器重新启动后重新建立连接。重新启动的持续时间主要取决于以下参数

- 数据结构的范围
- OPC UA 地址空间中可见的变量数
- 关于根据 OPC UA 规范 (<= V1.03) 向下兼容数据类型定义的设置（启用 TypeDictionary）

有关通信负载和最短循环时间设置的更多信息，请单击此处 (页 305)

对于 V2.8 以下的 CPU 固件版本，每次下载到 CPU 时 OPC UA 服务器都会停止，之后再重新启动。自固件版本 V2.8 起，OPC UA 服务器的行为已得到如下优化：在 CPU 的 STOP 操作状态下载对象时，OPC UA 服务器仍始终停止，之后再重新启动。在这种情况下，STEP 7 不会显示警告。在 CPU 的 RUN 操作状态下载对象时，OPC UA 服务器仅在加载的对象与 OPC UA 相关或者可能与之相关的情况下才会停止。由于 OPC UA 数据发生修改，OPC UA 服务器会在重新初始化后再重新启动。在将 OPC-UA 相关对象加载到 CPU 并停止 OPC UA 服务器之前，STEP 7 会在加载预览对话框中显示警告。随后，用户可以决定是在完成下载操作后重新启动服务器，还是取消下载操作。这类警告仅在 OPC UA 服务器运行时显示。如果 OPC UA 服务器未启用，修改后的 OPC UA 数据对下载过程没有影响。示例 只需要向程序中添加其他代码模块。数据块以及输入、输出、标记、时间或计数器均不受影响。加载期间的反应：正在运行的 OPC UA 服务器不中断。需要加载新数据模块并将数据模块标记为非 OPC-UA 相关：加载期间的反应：正在运行的 OPC UA 服务器不中断。需要覆盖数据模块。加载期间的反应：显示警告，提示您服务器即将重启。背景：STEP 7 无法确定更改是否与 OPC-UA 数据相关。通过 OPC UA 服务器读取 CPU 的操作模式通过 OPC UA 服务器可读出 CPU 模式