

西门子PLC模块授权总经销商 6ES7134-6FF00-0AA1 ET 200SP 模拟式输入端模块

产品名称	西门子PLC模块授权总经销商 6ES7134-6FF00-0AA1 ET 200SP 模拟式输入端模块
公司名称	浔之漫智控技术(上海)有限公司
价格	.00/件
规格参数	西门子:全国授权销售 ET200SP:全新 德国:现货
公司地址	上海市松江区石湖荡镇塔汇路755弄29号1幢一层 A区213室
联系电话	15801997124 15801997124

产品详情

西门子PLC模块授权总经销商 6ES7134-6FF00-0AA1 ET 200SP 模拟式输入端模块

6ES7134-6FF00-0AA1

SIMATIC ET 200SP，模拟式输入端模块，模拟输入
8XU 基础型，适合用于 A0 类型的基座单元，A1，
颜色代码 CC02，模块诊断，16 位

要连接到 OPC UA 服务器，OPC UA 客户端需要其端点的相关信息，如端点 URL 和安全策略。如果网络中提供大量可用服务器，则发现服务器可负责处理对该服务器信息的搜索和管理。OPC UA 服务器注册使用发现服务器。OPC UA 客户端向发现服务器请求获取可访问的服务器列表，然后连接到所需 OPC UA 服务器。全球发现服务器 (GDS) OPC UA GDS 理念一方面可组态跨子网发现服务，另一方面为证书集中管理提供接口。全球发现服务器 (GDS) 提供的机制可实现对以下组件的集中管理：CA 签名证书和自签名证书受信任列表和证书吊销列表 (CRL) 因此，GDS 提供中央证书管理的接入点，并接管 OPC UA 网络中安全服务器的任务。GDS 主要用于通过相应的 CRL 来管理 CA 签名证书：首次创建 OPC UA 应用程序证书 定期更新受信任列表和 CRL 更新应用程序证书 证书管理 证书管理的任务是自动管理和分发不同服务器或 UA 应用程序的证书和信任列表。在该上下文中，有以下两种不同的角色：证书管理器 - 提供证书管理功能的 OPC UA 应用 证书接收方 - 从证书管理器接收证书、信任列表和 CRL 的 OPC UA 应用程序。证书管理分为以下两种模式：拉取管理和推送管理。采用拉取管理模式时，OPC UA 应用作为 GDS 服务器的客户端运行，并使用证书管理方法来请求获取证书更新和信任列表更新。采用推送管理模式时，OPC UA 应用作为服务器运行，并提供将 OPC UA GDS 用作 OPC UA

客户端的方法。充当证书管理器的 GDS 用此等方法传送（“推送”）证书和受信列表更新，有关概念说明，请参见下文中的自动证书更新。目前，仅 S7-1500 CPU 固件版本 V2.9 及以上版本的 OPC UA 才支持推送管理。164 通信功能手册, 11/2022, A5E03735819-AK OPC UA 通信 10.2 OPC UA 的信息安全 使用 GDS 的系统组态 下图显示了与提供证书管理功能的 GDS 相关的各个设备的任务示例。

根 CA - 为系统颁发证书的设备（此等证书也可通过其它方式传送，例如通过电子邮件方式）

安装有证书管理器的 OPC UA GDS，可创建或签名设备证书、管理信任列表和证书吊销列表（CRL），以及将证书和列表写入设备中（推送功能）。对于推送功能，此设备需要 OPC UA 客户端功能。装有 OPC UA 应用的设备，接收“推送”的证书和列表 STEP 7 版本 V17

及更高版本的自动证书更新概念 GDS

和证书管理器通常合并到一个应用中，但下图中以两个独立的组件显示。“普通的” OPC UA 客户端之类的设备也可以用作证书管理器，但它们需要支持 Bytestring 数据类型才能传送证书，例如，固件版本为 V2.9 以及更高版本的 S7-1500 CPU 作为 OPC UA 客户端或者具有

GDS 插件的 UA Expert 工具 (Unified Automation)。S7-1500 CPU 的 OPC UA

服务器作为证书接收方，可提供 OPC UA 客户端证书读取和写入信任列表和 CRL

时所需的标准方法与属性。S7-1500 CPU 的 OPC UA 服务器上下文的侧重点是介绍如何使用推送功能为 CPU 提供证书，并与常规方法（通过下载硬件配置）进行了比较。下图显示了 S7-1500 CPU 固件版本 V2.9 或更高版本中 OPC UA 证书与列表的传输方式：或是在 CPU 处于 STOP

模式时，通过加载硬件配置来更新；证书是硬件配置的组成部分。或是在 CPU 处于 RUN 或 STOP

模式时，通过 GDS 推送方法来更新。165 OPC UA 通信 10.2 OPC UA 的信息安全 通信功能手册, 11/2022,

A5E03735819-AK 两种方法不能同时使用。如果选择在运行系统中通过 GDS 推送功能传送 OPC UA

服务器证书，则必须通过此途径将其它所有证书类型传送到 CPU。&\$ &HUWLILFDWH 'DWEDEVH 23& 8\$ 6HUYHU &HUWLILFDWHV 'RZQORDG +DUGZDUH FRQILJXUDWLRQ

&HUWLILFDWH 0DQDJHU &HUWLILFDWH 5HFHLYHU 23& 8\$ &OLHQW *HW /LVW 7UXVW 3XVK 8SGDWH &HUWLILFDWHV DQG 7UXVW /LVW 6 &38 *6 6,0\$7,& 0HPRU\

&DUG 7,\$ 3RUWDO 更多信息 有关 OPC UA 证书的更多信息，请参见“OPC UA 证书 (页

157)”部分。10.2.7.2 推送功能的组态限制 推送功能的证书数量在 S7-1500 CPU 固件版本 V2.9

及以上版本中，无论何种类型，OPC UA 推送功能的组态限值均为 62 个信任列表条目。

每个激活的基于证书的服务（CPU 应用程序）“消耗”一个证书条目和一个私钥条目。

证书吊销列表条目 (CRL) 的计数与受信任证书列表条目的计数方式一样。由不同服务（CPU

应用程序）使用的证书计为一个信任列表条目。推送功能的元素大小（例如证书）*多 4096 个字节

示例 希望授予*多 62 个 OPC UA 客户端对 OPC UA 服务器的访问权限，并相应填写受信任列表。

在受信任列表中添加“证书吊销列表”条目时，*多只能信任 61 个客户端证书。

不能通过将硬件配置下载到 CPU 来传输更多的 OPC UA 证书。提示

为了尽可能减少所需证书的数量，建议您通过同一个 CA 对 OPC UA 客户端证书进行签名。166 通信功能手册, 11/2022, A5E03735819-AK OPC UA 通信 10.2 OPC UA 的信息安全 在这种情况下，作为 OPC UA

服务器的 CPU 仅需要相应的 CA 证书和 CRL。通过这些元素，OPC UA 服务器随后可以验证由 CA

签名的所有客户端证书。即，无需将每个客户端证书逐一添加到受信任列表中。10.2.7.3 设置和下载

GDS 参数 下文介绍了证书更新的所需设置。要求 不同应用程序证书需要使用对应的 STEP 7/TIA Portal

版本和 S7-1500 CPU 固件版本。另请参见“证书管理的必备知识 (页 48)” – OPC UA

服务器证书需要使用 TIA Portal V17 及更高版本、CPU 固件版本 V2.9 – Web 服务器证书需要使用 TIA

Portal V18 及更高版本、CPU 固件版本 V3.0 已设置 CPU 的时间/日期（通常应用于基于证书的通信）

已启用 OPC UA 服务器。必须启用 GDS 推送管理使用的服务。例如，必须启用 Web 服务器才能传送

Web 服务器证书。至少必须组态一个采用“签名并加密”安全策略的端点。伙伴必须使用此端点。

已为经过身份验证的用户组态足够的功能权限 用户必须拥有具备“管理证书”功能权限的角色。

该功能权限具有以下要求： – 必须在项目树中启用项目保护：项目树：“安全设置 > 设置 >

项目保护” (Security settings > Settings > Project protection)。 – 在 CPU 设置的“CPU UA > 常规” (OPC UA

> General) 区域中，必须启用以下常规用户管理设置：“通过项目安全设置启用其它用户管理” (Enable

additional user management via project security settings) “具有 OPC UA 功能权限的用户和角色 (页

210)”部分介绍了如何设置功能权限。激活 GDS 满足上述要求后，仍必须启用 GDS：1.

在巡视窗口（CPU 参数）中，转到“OPC UA > 服务器 > 常规” (OPC UA > Server > General) 区域。2.

启用“启用全球发现服务（推送）” (Enable Global Discovery Services (Push)) 选项。

确定使用的证书存储区 使用 GDS 进行管理的证书与通过 TIA Portal (STEP 7)

下载的证书不在同一存储区中。 167 OPC UA 通信 10.2 OPC UA 的信息安全 通信 功能手册, 11/2022, A5E03735819-AK 启用 GDS 推送证书管理后, CPU

的服务 (应用程序) 同样使用该证书存储区中的证书, 这些证书可以在运行期间进行管理。 1. 在 CPU 设置中, 导航至 “保护与安全 > 证书管理” (Protection & Security > Certificate management) 区域。 2. 选择 “运行期间使用证书管理器提供的证书” (Use certificates provided by the certificate management at runtime) 选项。 另一种方式则使用从 TIA Portal 下载到 CPU 中的证书, 这些证书在 CPU 处于 STOP 模式时进行组态。该证书存储区中的证书或信任列表无法在运行时更新。 启用证书失效诊断 如果希望提前收到证书失效通知, 请在 “保护与安全 > 证书管理” (Protection & Security > Certificate management) 区域中选择 “启用证书失效系统诊断事件” (Enable system diagnostics event for the certificate lapsing) 选项。 在输入字段 “显示剩余证书有效期的事件:” (Show event at remaining certificate validity period of:) 输入百分比值。 这些设置的作用:

证书达到该值时, 将出现相应的系统诊断消息, 该消息在证书失效或刷新后才会消失。

如果证书已到期, CPU 将生成相应的系统诊断消息, 并在诊断缓冲区中生成一个条目, 且维护 LED 指示灯亮起。 示例: 在 2022 年 6 月 1 日通过 GDS 传送的证书的有效期为 2022 年 6 月 1 日至 2022 年 6 月 30 日 (30 天)。已在诊断事件中输入百分数值 10。2022 年 6 月 27 日, 90% 的有效期将到期。

此时, 将显示一条消息, 指示所传送的证书将于 2022 年 6 月 30 日到期。

无论组态的百分数值是多少, 证书的有效期到期后, 都将显示一条相应的消息并在诊断缓冲区中输入一个条目, 同时维护 LED 指示灯亮起。 下载到 CPU 将组态下载到 CPU 之前, 可删除由 GDS 管理的证书。确认删除后, 下载完成时将进入配置阶段 (参见调试部分)。 下载 CPU 之外的存储卡 (读卡器) 时, 始终会删除该证书存储区。

如果激活全球发现服务 (推送) 但未推送任何证书, 则 OPC UA 服务器上没有任何证书、信任列表或 CRL。 10.2.7.4 GDS 调试 OPC UA 规范第 12

部分对证书管理期间的配置阶段和运行阶段进行了区分定义。在配置阶段, GDS 或 OPC UA 客户端为 OPC UA 服务器的客户端提供初始信任列表和 CRL。在此阶段中, CPU 的 OPC UA

服务器接受提供的所有客户端证书和列表; 与 OPC UA 服务器的 “受

信任的客户端” 设置类似, 在运行期间接受所有客户端证书。服务器只能通过这种方式与未知客户端建立连接。例如, 客户端无法通过现有证书或信任列表进行身份验证, 而只能在接收相应的客户端证书或相应的信任列表后餐呢个进行验证。

配置阶段有信息安全水平低的特点; 因此, 配置阶段将通过点亮维护 LED 以及在相应的诊断缓冲区中记录条目 (需要维护) 的方式加以指示。在运行阶段中, 现有的 CRL

将进行更新 (举例而言), 并且证书和信任列表也将更新。通信在此阶段中是安全的。 168 通信 功能手册, 11/2022, A5E03735819-AK