西门子PLC模块授权总经销商 6ES7134-6HD01-0BA1 ET 200SP 模拟量输入标准型

产品名称	西门子PLC模块授权总经销商 6ES7134-6HD01-0BA1 ET 200SP 模拟量输入标准型
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 6ES7134-6HD01-0BA1 ET 200SP 模拟量输入标准型

6ES7134-6HD01-0BA1

SIMATIC ET 200SP, ANALOG INPUT MODULE, AI 4XU/I 2-WIRE STANDARD, PACKING UNIT: 1 PIECE, FITS TO BU-TYPE A0, A1, COLOR CODE CC03, MODULE DIAGNOSIS, 16BIT, +/-0,3%

OPC UA 通常采用数组访问方式进行读写操作问，即带有下标和长度。一个单变量实际上就是一各特殊的数组（下标为 0，长度为 1）。只是在该线路上重复发送此数据类型。对于变量，“ DataType ”属性指示基本数据类型。属性“ ValueRank ”和“ ArrayDimensions ”用于显示当前是否使用数组进行处理以及该数组的大小。 基于数组的数据类型 一些 SIMATIC 数据类型的 OPC UA 值映射到字节数组中。这些数据类型的数组随后会映射为二 维数组。 示例：SIMATIC 数据类型 DATE_AND_TIME (DT) 在 OPC UA 侧映射到 8 字节数组 (Byte[8])，见 上表。定义 SIMATIC 数据类型 DATE_AND_TIME (DT) 的数组时，会将其视为二维数组。 这会影响 OPC_UA_NodeAdditionalInfo 和 OPC_UA_NodeAdditionalInfoExt 系统数据类型的使 用，例如：
对于上述数据类型，必须为多维数组使用系统数据类型 OPC_UA_NodeAdditionalInfoExt，而 不是 OPC_UA_NodeAdditionalInfo。 结构 结构作为 ExtensionObject 进行传送。S7-1500 服务器使用二进制表示来在线路上传输 ExtensionObjects；各结构元素相继出现。在前面的是数据类型的 NodeId；客户端使用其来建 立结构。 对于 OPC UA 规范 V1.03 及以下版本，要实现该目的，客户端需读取、解码和解析完整的 DataTypeDictionary（除非已通过 XML

导入功能离线学习此库）。 从 OPC UA V1.04 开始，DataTypeDescription
属性也可用于此目的，即可以更快速轻松地进行
读取和解析。客户端仅在第一次访问期间或之前一次性确定结构设置，随后会在会话期间使用 此信息。
特殊 SIMATIC 数据类型 上表中不存在以及无法定义为结构或 PLC 数据类型元素的 SIMATIC
数据类型不受 OPC UA 客户 端支持。 举例来说，此类数据类型有 “ ANY ” 或 “ POINTER ” 指针、函数
块 “ Block_FB ” 、函数 “ Block_FC ” 或硬件 数据类型 “ REMOTE ” 。
如果选择不受支持的数据类型，则将生成一条错误消息。 更多信息
有关基本数据类型、数组和结构映射的更多详细信息，请参见 OPC UA 规范第 6 部分 “ 映 射 ” （参见
OPC UA BINARY）。 对于 SIMATIC S7-1500 OPC UA 服务器中的数组与数据类型 DTL 和
LDT，必须考虑哪些因素？ 常见问题解答 (https://support.industry.siemens.com/cs/cn/zh/view/109766726) 153
OPC UA 通信 10.1 需了解的 OPC UA 知识 通信 功能手册, 11/2022, A5E03735819-AK 10.2 OPC UA
的信息安全 10.2.1 安全设置 寻址风险 OPC UA
支持过程和生产层级中的不同系统之间以及这些系统与控制与企业层级中的系统之间 的数据交换。
这同样将导致信息安全风险。因此，OPC UA 提供了一系列安全防护机制： OPC UA
服务器和客户端的身份验证。 检查用户的身份。 在 OPC UA
服务器和客户端间，对已签名/加密的数据进行交换。 仅在**有必要的情况下，才应绕过这些安全策略：
调试过程中 在没有外部以太网连接的独立项目中 例如，如果 OPC Foundation 的 “ UA Sample
Client ” 端点选择了 “ 无 ” (None)，则程序将发出一条 明确的警告消息： STEP 7
编译项目时，还会检查用户是否考虑保护设置选项，并会警告用户可能存在的风险。
还包括采用 “ 不安全 ” (no security) 设置的 OPC UA 安全策略，该设置对应于端点 “ 无 ” (None)。 说明
禁用不需要的安全策略 如果在 S7-1500 OPC UA
服务器的安全通道设置中启用了所有安全策略，即采用端
点 “ 无 ” (None)（不安全），则服务器和客户端之间还可能存在非安全数据通信（既未签名也未
加密）。S7-1500 CPU 的 OPC UA 服务器还会向设置为 “ 无 ” (None)（不安全）的客户端发送公
用证书。某些客户端会检查该证书。但不会强制客户端向服务器发送证书。客户端的身份可能
仍保持未知。无论后续为哪种安全设置，每个 OPC UA 客户端随后都可以连接到服务器。 组态 OPC UA
服务器时，请确保只选择与您的设备或工厂的安全概念兼容的安全策略。应禁用 所有其它安全策略。
建议：使用 “ Basic256Sha256 - 签名和加密 ” (Basic256Sha256 - Sign and Encrypt) 设置，说明 服务器只接受
Sha256 证书。安全策略 “ Basic128Rsa15 ” 和 “ Basic256 ” 默认取消激活，不能用作
端点。请选择安全策略较高的端点。 附加安全规则 仅在特殊情况下，使用端点 “ 无 ” (None)。
仅在特殊情况下，使用 “ 访客身份验证 ” 。 如果确实有必要，则仅允许通过 OPC UA 访问 PLC 变量和
DB 元素。 在 S7-1500 OPC UA 客户端的设置中使用可信客户端列表，以仅允许对特定客户端进行访 问。
154 通信 功能手册, 11/2022, A5E03735819-AK OPC UA 通信 10.2 OPC UA 的信息安全 10.2.2 ITU X.509 证书
OPC UA 的多个层级中，都集成有安全机制。其中，数字证书至关重要。仅当 OPC UA 服务器 接受 OPC
UA 客户端的数字证书并将其归类为可信时，客户端才能与服务器建立安全连接。
请参见 “ 处理客户端和服务器证书 (页 202) ” 部分。
与此同时，客户端还必须检查并信任服务器的证书。服务器和客户端必须显示自己的身份，并
证明该身份与声明的相同：即，服务器和客户端必须证明自己的身份。例如，客户端和服务器
的相互验证可有效防止中间人攻击。 “ 中间人 ” 攻击
“ 中间人 ” 可能会出现在服务器和客户端之间。中间人是一种程序，会截获服务器与客户端之间
的通信并将自身伪装为客户端或服务器，以获取 S7 程序的相关信息或设置 CPU 的值，进而对
设备或工厂进行攻击。 OPC UA 使用的数字证书符合国际电信联盟 (ITU) 的 X.509 标准，
可识别（认证）一个程序、计算机或机构的身份。 X.509 证书 X.509 证书包含以下信息： 证书的版本号
证书的序列号 证书颁发机构对证书进行签名的算法。 证书颁发机构的名称
证书有效期的起始和结束时间 由证书颁发机构签名证书的程序、个人或机构名称。
程序、个人或机构的公钥。 因此，X509
证书将身份（程序、个人或机构的名称）与该程序、个人或机构的公钥关联在一 起。
在连接建立期间检查
客户端与服务器建立连接时，设备将基于证书检查全部所需信息以确保其完整性，如签名、有
效期、应用程序名称 (URN)，对于固件版本 V2.5，还会检查客户端证书中客户端的 IP 地址。 说明
此外，还会检查证书中存储的有效期。因此必须设置 CPU 时钟，且日期/时间必须在有效期

内，否则将无法进行通信。 签名和加密 要检查证书是否篡改，则需对证书进行签名。 155 OPC UA 通信 10.2 OPC UA 的信息安全 通信 功能手册, 11/2022, A5E03735819-AK 可通过以下几种方式进行操作： 在 TIA Portal 中，可生成证书并为证书签名。如果您已对项目进行保护，并以具有可进行安全设置的功能权限的用户身份登录，则可以使用全局安全设置。通过全局安全设置可访问证书管理器，由此也可访问 TIA Portal 的证书颁发机构 (CA)。
还可通过其它选项创建证书并为证书签名。在 TIA Portal 中，可将证书导入到全局证书管理 器中。 – 联系一家证书颁发机构 (CA) 并对证书进行签名。
此时，认证颁发机构将核实您的身份，并通过该证书颁发机构的私钥对您的证书进行签名。为此，需向证书颁发机构发送一个 CSR（证书签名请求）。 – 自行创建证书并对其进行签名。
例如，为实现上述过程，您应使用 OPC 基金会的 “ Opc.Ua.CertificateGenerator ” 程序。 还可使用 OpenSSL。 有关更多信息，请参见 “ 用户自己生成 PKI 密钥对和证书 (页 158) ” 。 有用信息：证书类型 自签名证书 每个设备都可生成并签署自己的证书。应用示例：通信节点数量有限的静态组态。
不能从自签名证书派生新的证书。但是，需要将所有自签名证书从伙伴设备加载到 CPU（需要在 STOP 模式下执行）。 CA 证书： 所有证书都由证书颁发机构生成和进行签名。应用示例：动态添加设备。
只需将证书从证书颁发机构下载到 CPU。证书颁发机构可以生成新的证书（添加伙伴设备 无需在 CPU STOP 模式下）。 签名 如下所述，通过该签名，可验证消息的完整性和来源。
首先，发送方根据纯文本信息（纯文本消息）生成 HASH 值。之后，再通过私钥对该 HASH 值进行加密，并将该纯文本消息连同加密后的 HASH 值一同发送到接收方。验证签名时，接收方需要一个发送方的公钥（包含在发送方的 X509 证书中）。接收方基于发送方的公钥，对接收 到的 HASH 值进行解密。然后，接收方再根据接收到的纯文本消息生成自己的 HASH 值 （HASH 过程包含在发送方的证书中）。接收方对这两个 HASH 值进行比较： 如果两个 HASH 值相同，则表示从发送方接收到的纯文本消息未经更改并未被篡改。 如果两个 HASH 不匹配，则表示到达接收方的的纯文本消息发生了更改。纯文本消息在传 送过程中被篡改或受损。 加密 加密数据可防止非经授权的读取。X509 证书不加密；这些证书为公开证书，任何人均可查 看。
在加密过程中，发送方将使用接收方的公钥对纯文本消息进行加密。为此，发送方需要接收方 的 X509 证书。这是因为，该证书中包含接收方的公钥。接收方使用自己的私钥对消息进行解密。只有接收方才能对该消息进行解密：只有他们才拥有相应的私钥。因此，任何时候私钥都不得泄露。 156 通信 功能手册, 11/2022, A5E03735819-AK OPC UA 通信 10.2 OPC UA 的信息安全 安全通道 OPC UA 使用客户端与服务器的私钥和公钥建立安全连接，即安全通道。建立安全连接后，客户端和服务器将生成一个只有它们才了解的内部密钥，它们使用此密钥对消息进行签名和加密。较非对称加密过程（私钥和公钥）过程，对称加密过程（共享密钥）的运行速度要快得 多。
更多信息 有关通过 TIA Portal 使用证书的应用示例，请参见此处：通过 TIA Portal使用证书 (https://support.industry.siemens.com/cs/ww/zh/view/109769068)。 10.2.3 OPC UA 证书 使用 OPC UA 的 X509 证书 OPC UA 可使用各种类型的 X.509 证书在客户端与服务器之间建立连接： OPC UA 应用程序证书 这类 X.509 证书用于标识软件实例、客户端或服务器软件的安装。在 “ 机构名 称 ” (Organization name) 属性中，可输入该软件使用方的名称。 说明 即使安全设置为 “ 无 ” (None)（不安全），S7-1500 的 OPC UA 服务器也会使用应用程序证 书。这可保证与 OPC UA V1.1 及更早版本的兼容性。 OPC UA 软件证书 X-509 证书用于标识客户端或服务器软件的特定版本。这些证书中包含有关属性，用于说 明通过 OPC 基金会（或认可的测试实验室）认证时的软件版本。在 “ 机构名 称 ” (Organization name) 属性中，可输入该软件的研发或销售方名称。 说明 STEP 7 不支持软件证书。 OPC UA 用户证书 该 X.509 证书用于标识特定用户，例如从 OPC UA 服务器检索过程数据的用户。如果用户可通过密码自行认证或组态为匿名访问，则无需使用该证书。 说明 STEP 7 不支持用户证书。
所述证书属于*底层实体证书：这些证书用于识别个人、机构、公司或软件实例（安装）等信 息。