SIEMENS西门子 3VA1 IEC断路器 3VA11966ED320AA0

产品名称	SIEMENS西门子 3VA1 IEC断路器 3VA11966ED320AA0
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:代理经销商 低压断路器:全新原装 假一罚十 德国:正品现货 实体经营
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	15801815554 15801815554

产品详情

S7-1500 CPU（作为 TLS 服务器）与外部 PLC（TLS 客户端）之间的安全 OUC 在以下章节中，将介绍如何通过 TCP 建立 S7-1500 CPU（作为 TLS 服务器）与 TLS 客户端之间的开放式用户通信。 通过通信伙伴的域名建立 TCP 安全连接。 S71500 CPU 固件版本 V2.0 及以上版本支持通过域名系统 (DNS) 进行寻址的安全通信。 要通过域名进行 TCP 安全通信，则需手动创建一个 TCON_QDN_SEC 系统数据类型的数据块， 并分配参数，之后在 TSEND_C、TRCV_C 或 TCON 指令中直接调用该数据块。 要求： 在 CPU 中，设置当前的日期和时间。 网络中包含至少一台 DNS 服务器。 已为 S7-1500 CPU 组态至少一台 DNS 服务器。 TLS 客户端和 TLS 服务器具有所需的全部证书。 要建立与 TLS 客户端的安全 TCP 连接，请按以下步骤操作： 1. 在项目树中，创建一个全局数据块。2. 在该全局数据块中，定义一个 TCON_QDN_SEC 数据类型的变量。 在以下示例中，显示了一个全局数据块 “ Data_block_1 ”，其中，定义了数据类型 TCON_QDN_SEC 的变量 “ DNS ConnectionSEC ”。3. 在 “ 起始值 ” (Start value) 列中，设置 TCP 连接的连接参数。例如，在 “ ID ” 中输入 TCP 连接的 本地 ID。 4. 在 “ 起始值 ” (Start value) 列中，设置安全通信的参数。 – “ ActivateSecureConn ”：激活该连接的安全通信。如果该参数的值为 FALSE，则忽略后 面的安全参数。此时，可建立非安全的 TCP 或 UDP 连接。 – “ TLSServerReqClientCert ”：TLS 客户端需具有 X.509-V3 证书。 – “ TLSServerCertRef ”：自身 X.509-V3 证书的 ID。 “ TLSClientCertRef ”：X.509-V3 证书（或 X.509-V3 证书组）的 ID，TLS 服务器使用该 ID 验证 TLS 客户端的身份。如果该参数为 0，则 TLS 服务器将使用服务器证书中心当前加 载的所有 (CA) 证书对客户端的身份进行验证。 5. 在程序编辑器中，创建一个 TSEND_C、TRCV_C 或 TCON 指令。有关 TCON_QDN_SEC 系统数据类型的更多信息，请参见 STEP 7 在线帮助。 有关安全通信的更多信息，请参见 “ 安全通信 (页 40) ” 部分。 两个 S7-1500 CPU 之间的安全 OUC 在以下章节中，介绍如何通过 TCP 在两个 S7-1500 CPU 之间建立开放式用户安全通信。在此过程中，一个 S71500 CPU 用作 TLS 客户端（主动建立连接）而另一个 S71500 CPU 则用作 TLS 服务器（被动建立连接）。 建立两个 S7-1500 CPU 之间的安全 TCP 连接 要在两个 S71500 CPU 之间建立

TCP 安全通信，则需为每个 CPU 手动创建 TCON_IP_V4_SEC
系统数据类型的数据块，并分配相应参数，之后在 TSEND_C、TRCV_C 或 TCON 指令中直接调用该数据块。 要求： 在 CPU 中，设置当前的日期和时间。 两个 S71500 CPU 的固件版本为 V2.0 及以上版本TLS 客户端的设置 要在 TLS 客户端中建立安全的 TCP 连接，请按以下步骤操作： 1. 在项目树中，创建一个全局数据块。 2. 在该全局数据块中，定义一个数据类型为 TCON_IP_V4_SEC 的变量。 以下示例中显示了全局数据块“ Data_block_1 ”，其中，定义了数据类型为 TCON_IP_V4_SEC 的变量“ SEC 连接 1 TLS 客户端 ”(SEC connection 1 TLS-Client)。

3. 在“ 起始值 ”(Start value) 列中，设置 TCP 连接的连接参数。例如，在“ RemoteAddress ”中输 入 TLS 服务器的 IPv4 地址。 说明 连接参数接口 ID 请注意，可为数据类型为 TCON_IP_V4_SEC 的接口 ID 输入值“ 0 ”。在这种情况下，CPU 会自行搜索合适的本地 CPU 接口。 4. 在“ 起始值 ”(Start value) 列中，设置安全通信的参数。 – “ ActivateSecureConn ”：激活该连接的安全通信。如果该参数的值为 FALSE，则忽略后面的安全参数。此时，可建立非安全的 TCP 或 UDP 连接。 – “ TLSServerCertRef ”：输入值“ 2 ”（引用 TIA Portal 项目 (SHA256) 的 CA 证书），或输入值“ 1 ”（引用 TIA Portal 项目 (SHA1) 的 CA 证书）。如果使用不同的 CA 证书，则需在证书管理器的全局安全设置中输入相应的 ID。 – “ TLSClientCertRef ”：自身 X.509-V3 证书的 ID。 5. 在程序编辑器中，创建一个 TSEND_C、TRCV_C 或 TCON 指令。 6. 将 TSEND_C、TRCV_C 或 TCON 指令的 CONNECT 参数与 TCON_IP_V4_SEC 数据类型的变 量进行互连。 TLS 服务器的设置 要在 TLS 服务器中建立安全的 TCP 连接，请按以下步骤操作： 1. 在项目树中，创建一个全局数据块。 2. 在该全局数据块中，定义一个数据类型为 TCON_IP_4_SEC 的变量。
以下示例中显示了全局数据块“ Data_block_1 ”，其中，定义了数据类型为 TCON_IP_V4_SEC 的变量“ SEC 连接 1 TLS 服务器 ”(SEC connection 1 TLS-Server)。3. 在“ 起始值 ”(Start value) 列中，设置 TCP 连接的连接参数。例如，在“ RemoteAddress ”中输 入 TLS 客户端的 IPv4 地址。 4. 在“ 起始值 ”(Start value) 列中，设置安全通信的参数。 – “ ActivateSecureConn ”：激活该连接的安全通信。如果该参数的值为 FALSE，则忽略后面的安全参数。此时，可建立非安全的 TCP 或 UDP 连接。 – “ TLSServerReqClientCert ”：TLS 客户端需具有 X.509-V3 证书。输入值“ true ”。 – “ TLSServerCertRef ”：自身 X.509-V3 证书的 ID。 – “ TLSClientCertRef ”：输入值“ 2 ”（引用 TIA Portal 项目 (SHA256) 的 CA 证书），或输入值“ 1 ”（引用 TIA Portal 项目 (SHA1) 的 CA 证书）。如果使用不同的 CA 证书，则需在证书管理器的全局安全设置中输入相应的 ID。 5. 在程序编辑器中，创建一个 TSEND_C、TRCV_C 或 TCON 指令。 6. 将 TSEND_C、TRCV_C 或 TCON 指令的 CONNECT 参数与 TCON_IP_V4_SEC 数据类型的变 量进行互连。 在以下示例中，TSEND_C 指令的 CONNECT 参数将与变量“ SEC connection 1 TLS client ”（数据类型 TCON_IP_4_SEC）进行互连。通过 CP 接口进行安全 OUC 连接
在以下章节中，将介绍通过 CP 接口进行开放式用户安全通信时应注意的特殊事项。至少一个 站为 S7-1500 站，并包含以下模块： S7-1500 CPU 固件版本 V2.0 及以上版本（S7-1500 软件控制器除外） CP 1543-1 固件版本 V2.0 及以上版本，或 CP 1543SP-1 V1.0 及以上版本 该 CP 在 S7-1500 站中将作为 TLS 客户端（主动建立连接）或 TLS 服务器（被动建立连接）。 通过 CP 接口进行安全通信的基本操作步骤与概念，与通过 S7-1500 CPU 接口进行安全通信的类似。在此，必须将证书分配给作为 TLS 服务器或 TLS 客户端的 CPU，而非其它 CPU。因此，也可使用其他角色和操作步骤。在下文中，将对此进行详细介绍。管理 CP 的证书
以下规则普遍适用：在入全局安全设置中，需登录证书管理器。生成自签名的证书时，需登录全局安全设置。需要具有足够的用户权限（管理员权限，或具有“ 安全组态 ”权限的“ 标准 ”用 户）。在 CP 中，可在“ 安全 > 安全属性 ”(Security > Security properties) 部分生成或分配证书。在此部分中，可登录全局安全设置。 操作步骤： 1. 在 STEP 7 的网络视图中，选中该 CP 并在巡视窗口中选择“ 安全 > 安全属性 ”(Security > Security properties) 部分。 2. 单击“ 用户登录 ”(User logon) 按钮。 3. 使用用户名和密码进行登录。 4. 启用“ 激活安全功能 ”(Activate security functions) 选项。系统将初始化相应的安全属性。 5. 单击“ 设备证书 ”(Device certificates) 表格的第一行，生成一个新的证书或选择现有的设备证 书。 6. 如果通信伙伴也是一个 S7-1500 站，则需按照上述操作，使用 STEP 7 为通信伙伴或该 S7-1500 CPU 指定一个设备证书。 示例：通过 CP 接口，在两个 S7-1500 CPU 之间建立 TCP 安全连接 要在两个 S71500 CP 之间建立 TCP

安全通信，需为每个 CPU 手动创建 TCON_IP_V4_SEC 系统
数据类型的数据块，并分配相应参数，之后在 TSEND_C、TRCV_C 或 TCON 指令中直接调用该
数据块。 要求： 这两个 S7 1500 CPU 的固件版本为 V2.0 及以上版本如果使用 CP 1543SP-1：固件 V1.0
及 以上版本。 这两个 CP（如 CP 1543-1）的固件版本必须 V2.0 及以上版本 TLS 客户端和 TLS
服务器具有所需的全部证书。 – 必须为该 CP 生成设备证书（最终实体证书）并存储在该 CP
的证书存储器中。如果通信 伙伴是一个外部设备（如，MES 或 ERP
系统），则需确保该设备上包含有设备证书。 – 对通信伙伴设备证书进行签名的 root 证书（CA
证书）也必须位于该 CP 的证书存储器
中，或位于外部设备的证书存储器中。如果使用中间证书，则必须确保所验证设备中的
证书路径完整。设备将通过这些证书验证通信伙伴的设备证书。 这些通信伙伴需通过 IPv4
地址进行寻址，而不能通过域名进行寻址。