SIEMENS西门子 混合连接器电缆 6FX3802-7CD01-1CA0

产品名称	SIEMENS西门子 混合连接器电缆 6FX3802-7CD01-1CA0
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:原装正品 驱动器电机电缆:假一罚十 德国:现货包邮
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

分配 Windows 计算机名称时请遵循以下建议： 只能使用大写字母。
第一个字符必须为字母。 计算机名称的前 12 个字符必须唯一。 激活远程通信 在 WinCC
系统上，安装后默认禁用对话框 “ Simatic Shell ” 中的远程通信。对于以下应用，必
须激活所涉及计算机的远程通信： 将 Runtime 下载到其它 PC 上 客户端至服务器通信 冗余系统 WinCC
选件 “ WebNavigator ” 如果 WebNavigator 客户端与 WebNavigator
服务器未在同一计算机上运行，则必须激活 远程通信。 要启用远程访问，请按以下步骤操作： 1. 使用
Simatic Shell 的快捷菜单打开 Windows 资源管理器中的通信设置。 2. 激活 “ 远程通信 ” (Remote
communication) 选项。 3. 在网络中组态加密通信：选择预共享密钥和端口。 4.
选择网络适配器和（如有必要）多播设置。 取消激活 NTLMv1 和 SMBv1 可禁用 NTLMv1 和 SMBv1
协议。取消激活这两个协议不会对 WinCC Runtime Professional 的 操作产生任何影响。 说明 NTLMv1 和
SMBv1 带来的安全风险 使用 NTLMv1 和 SMBv1
协议会带来重大的安全风险。网络通信可能会因中间人攻击等受到 影响。
取消激活协议的步骤与具体的操作系统相关。

删除 SQL 实例 内容 安装 WinCC V19 后，会安装新的 Microsoft SQL Server 2019 实例。
如果您已经安装了 WinCC Runtime Professional 版本，则有以下选项： 在开始安装 WinCC Professional V19
之前，请先安装 WinCC Runtime Professional V19。 卸载 SQL Server 的旧 “ WINCC ” 实例。 说明 删除
WinCC Runtime Professional 或 WinCC Professional 时，不会删除 SQL 服务器中的实例。 卸载 SQL 实例 1.
打开 “ 控制面板 ” (Control Panel)。 2. 单击 “ 删除程序 ” (Remove program)。 3.
在已安装程序列表中，选择要移除的 Microsoft SQL Server 版本，然后单击 “ 移除/更
改 ” (Remove/change)。 4. 单击对话框中的 “ 移除 ” (Remove)。 5. 在 “ 选择实例 ” (Select instance)
对话框中，选择实例 “ WINCC ”，然后单击 “ 下一步 ” (Next)。 6. 在 “ 选择功能 ” (Select functions)
对话框中，单击 “ 全选 ” (Select all)，然后单击 “ 下一 步 ” (Next)。 7. 在 “ 功能规则 ” (Function

rules)对话框中，单击“ 下一步 ”(Next)。 8. 在“ 准备卸载 ”(Ready to uninstall)
对话框中，单击“ 移除 ”(Remove)。 9. 移除完成后，在“ 已完成 ”(Completed)
对话框中单击“ 关闭 ”(Close)。 卸载另一个版本的 SQL Server 实例的过程类似。有关安装 TIA Portal Teamcenter Gateway 的注意事项 简介 可通过以下方式安装 TIA Portal Teamcenter Gateway： 随 TIA Portal 一同安装 说明 安装服务器时，需要具有管理员权限。 安装要求 计算机上必须： 安装有 Teamcenter Rich Application Client（下文中称为“ RAC ”）或 Teamcenter Client Communication System (TCCS) 版本 V11.2 或更高版本。 说明 如果 TCCS 安装为“ 单机版 ”，则还需安装“ Microsoft Visual C++ 2013 – Redistributable ”。这样，可确保 TIA Portal 与 TIA Portal Teamcenter Gateway 之间建立有 连接。 FCC/FMS (FileClientCache/FileManagementSystem) 与“ Teamcenter Server 11.2 或更高 版本 ”之间存在连接 说明 重新安装或重启后，需检查 FCC/FMS (FileClientCache/FileManagementSystem) 与“ Teamcenter Server 11.2 或更高版本 ”之间是否存在连接。
重新安装或重启后，检查注册表项。有关检查注册表项的更多信息，请参见“ TIA Portal Teamcenter Gateway ”在线帮助中的“ 安装与卸载 TIA Portal Teamcenter Gateway > 检查 of TIA Portal Teamcenter Gateway 的安装 ”部分。 重新安装或重启后，需检查是否可在 Teamcenter
中保存条目类型以及是否可将数据集添
加到元素修订版中。有关保存元素类型的更多信息，请参见“ TIA Portal Teamcenter Gateway ”在线帮助中“ 通过 TIA Portal Teamcenter Gateway 管理 TIA Portal 项目 ”章节的“ 在 Teamcenter 中将 TIA Portal 项目另存为一个新条目 ”部分。 重新安装或重启后，检查是否可从 Teamcenter Rich Application Client 向 Teamcenter 服 务器传送数据。 Teamcenter 服务器上安装有所提供的 Teamcenter 数据模型（含多个文件）。安装 TIA Portal Teamcenter Gateway - 数据模型 安装所提供的 TIA Portal Teamcenter Gateway 数据模型时，需使用“ 系统管理 器 ”(Environment Manager)。
有关安装的说明，请参见产品 DVD 中的目录“ \Support\Teamcenter_11\ServerSetupDocument\ ”。
安装过程中，TIA Portal 的版本相同 安装不同的 TIA Portal
产品时，请确保安装时所用的服务包和更新版本相同。 例如，如果安装有 TIA Portal V14 或更高版本，则还需安装 TIA Portal Teamcenter Gateway V14 或更高版本。 安装路径
在安装路径中，请勿使用任何 UNICODE 字符（如，中文字符）。 防病毒程序
在安装过程中，需要对安装的文件进行读写访问。有些防病毒程序可能会阻止对这些文件进行访问。因此，建议在安装 TIA Portal Teamcenter Gateway 时禁用防病毒程序，并在安装后 重新启用。

TIA Portal 中的安全日志记录 TIA Portal
中的安全日志记录功能用于从工程组态系统以及自动化环境的组件中获取安全相
关事件和日志数据，并进行保存和分析。 事件和日志数据存储在本地 Windows 系统中。可通过 Windows 事件查看器对此类数据进行 分析、保存和导出。 可通过后续操作步骤将事件和日志数据传送到 SIEM 系统（安全信息和事件管理，Security Information and Event
Management）。因此，安全日志记录可从网络中的不同系统采集安
全相关数据并进行分析，并对威胁作出响应。安全日志记录是众多国际安全标准和规范推荐
的一系列安全措施之一，用于提高系统安全性。 TIA Portal
中默认禁用安全日志记录。初始状态下，管理员可通过批处理文件激活安全日志
记录。安全日志记录激活后，可通过批处理文件或 Windows 注册表禁用和重新激活。 参见 激活和取消激活安全日志记录 (页 75)激活和取消激活安全日志记录 将 TIA Portal
安装到计算机时，将注册安全日志记录的事件通道；但此功能默认处于禁用状 态。在 Windows 注册表的“ AuditLogOn ”键值中设置相应值，以激活和取消激活安全日志记
录。键值设置为“ 1 ”将激活安全日志记录，设置为其它键值将取消激活此功能。TIA Portal 中默认禁用安全日志记录。 “ AuditLogOn ”键值不是在安装 TIA Portal 时创建的。TIA Portal
安装目录的“ bin ”文件夹中有两 个批处理文件：
批处理文件“ SecurityAuditLoggingEnable.bat ”可创建“ AuditLogOn ”键值和激活安全日志记 录。
批处理文件“ SecurityAuditLoggingDisable.bat ”可取消激活安全日志记录。
安全日志记录与特定版本相关。该设置对 TIA Portal 的其它版本没有任何影响。要求 具有 Windows 管理员权限。 要登录用户帐户，项目必须受到保护。 通过批处理文件激活安全日志记录 1. 导航至 TIA Portal 安装目录的“ bin ”文件夹。 2. 运行批处理文件“ SecurityAuditLoggingEnable.bat ”。
通过批处理文件取消激活安全日志记录 1. 导航至 TIA Portal 安装目录的“ bin ”文件夹。 2.

运行批处理文件“ SecurityAuditLoggingDisable.bat ”。 在 Windows 注册表中激活和取消激活安全日志记录
1. 在 Windows 中打开注册表编辑器。 2. 转到键值
“ HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Automation\SecurityLogging\18.0\Settings\A
uditLogOn ”。 3. 要激活安全性日志记录，在“ LoggingOn ”键值中输入值“ 1 ”。
要取消激活安全性日志记录，在“ LoggingOn ”键值中删除或更改值“ 1 ”。 4. 单击“ 确定 ”(OK)
确认输入。 参见 TIA Portal 中的安全日志记录 (页 75) 事件概述 (页 76) 6.3 事件概述
下表简要列出了用户操作、相关日志条目、事件类别和事件类型：
除了下列表格中列出的事件内容，每个事件还包含以下信息： TIA Portal 的版本 项目的名称
用户管理（UMAC - 用户管理和访问控制）中已登录用户的用户名