西门子授权低压断路器中国经销商

产品名称	西门子授权低压断路器中国经销商
公司名称	湖南西控自动化设备有限公司
价格	.00/件
规格参数	
公司地址	中国（湖南）自由贸易试验区长沙片区开元东路1306号开阳智能制造产业园（一期）4#栋301
联系电话	15344432716 15386422716

产品详情

西门子授权低压断路器中国经销商

变频器； S120 V90 伺服控制系统；6EP电源；电线；电缆；

网络交换机；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。西门子中国有限公司授权合作伙伴——浔之漫智控技术(上海)有限公司，作为西门子中国有限公司授权合作伙伴，湖南西控自动化设备有限公司代理经销西门子产品供应全国，西门子工控设备包括S7-200SMART、S7-200CN、S7-300、S7-400、S7-1200、S7-1500、S7-ET200SP 等各类工业自动化产品。公司国际化工业自动化科技产品供应商，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。

西门子中国授权代理商——湖南西控自动化设备有限公司，本公司坐落于湖南省中国（湖南）自由贸易试验区长沙片区开元东路 1306 号开

阳智能制造产业园一期 4 栋 30市内外连接，交通十分便利。

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。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。

错误/故障 如果故障无法消除，请将设备送至西门子代表处进行维修。不允许现场维修。 1.9 解除调试

正确关闭设备，以防止未经授权的人员访问设备内存中的机密数据。

为此，需要恢复设备的出厂设置。回收和处置 该产品的污染物含量低，可以回收利用并且符合 WEEE

指令 2012/19/EU 对电子电气设备的 处置要求。 请勿将产品丢弃在公共场所。

为了使旧设备的回收和处置更符合环境要求，请联系一家经认证的电子废料处理公司或联系

西门子的联系人（产品回收）。 请注意不同国家的法规。 1.11 商标

以下所列名称以及其它可能的名称虽然不带注册商标符号，但它们均为 Siemens AG 的注 册商标：

SCALANCE SINEC 1.12 静电放电 注意 静电敏感设备 (ESD) 电子模块包含静电敏感元件

如果处理不当，这些元件很容易受到损坏。 为避免损坏，请注意以下说明。

只能在必须使用电子模块的情况下才能触摸此类模块。

如果需要触摸电子模块，则相关人员的身体必须先释放静电并且处于接地状态。

请勿使电子模块与电气隔离型材料（例如塑料薄膜、隔离工作台衬垫或合成纤维制成的布料） 接触。

仅将模块置于导电表面。

只能使用导电的包装材料（例如，涂有金属的塑料或金属容器、导电海绵或者家用铝箔）来

包装、存储和运输电子模块。读安全注意事项

请注意以下安全注意事项。这与设备的整个工作寿命有关。

您还应该阅读各部分（尤其是“ 安装 ”和“ 连接 ”部分）中与处理相关的安全注意事项。 小心

为防止人员受伤和产品损坏，请在使用设备前阅读本手册。 有关在危险场所使用的安全注意事项

与防爆相关的通用安全注意事项 警告 爆炸危险 请勿在接通电源的情况下打开设备。 符合 UL/FM HazLoc

要求的危险场所使用安全须知 如果在 UL 或 FM HazLoc

条件下使用设备，除了防爆通用安全须知外，还必须遵守以下安全 须知： 此设备仅适合在 I 类，2

分区，A、B、C 和 D 组或无危险位置使用。 此设备仅适合在 I 类，2 区，IIC 组或无危险位置使用。注意

信息安全 在运行设备之前，连接设备并更改出厂时设置的用户“ admin ”和“ ”的标准密码。 3.1

安全建议 为防止设备和/或网络受到未经授权的访问，请遵循以下安全建议。 常规

定期检查设备，确保其符合以下建议和/或任何内部安全政策。

评估站点安全性，并将单元保护机制与适当的产品配合使用： 更多相关信息查看与设备一起使用的其它

Siemens 产品的用户文档，以获取更多安全建议。

使用远程系统记录将系统日志转发到中央记录服务器。确保服务器位于受保护的网络内，

并定期检查日志，以识别潜在的安全违规情况/漏洞。 有关详细信息，请参见 “ 补充文档 (页 8) ” 。

验证 注意 访问危险 - 数据丢失风险

请勿泄露设备的密码。只能通过将设备复位为出厂默认设置（这会删除所有组态数据）来

恢复对设备的访问。

部署设备之前，请更换所有用户帐户、访问模式和应用程序（如适用）的默认密码。

使用密码强度高的密码避免使用密码强度弱的密码（如，password1、123456789、

abcdefgh）或重复字符（如，abcabc）。 此建议也适用于对设备组态的对称密码/密钥。

确保密码受到保护，切勿分享给未授权人员。 请勿为不同的用户名和系统重复使用相同的密码。请将密

码记录在安全的离线位置，以供今后忘记密码时查阅。 经常定期更改密码。 如果使用 RADIUS

进行用户身份验证，请确保所有通信都在安全边界范围内或受到安全通 道保护。

注意在端点之间不提供任何内在身份验证的链路层协议，例如 ARP 或 IPv4。恶意实体可

利用这些协议中的漏洞来攻击连接到第 2 层网络的主机、交换机和路由器，例如，通过 使子网中系统的

ARP 缓存中毒并随后拦截数据流量。为防止对网络进行未授权访问，应 针对非安全第 2

层协议采取适当的保护措施，比如保护对本地网络的物理访问或使用安 全的上层协议。 证书和密钥

如果怀疑存在安全违规，请立即更改所有证书和密钥。 管理员用户可访问 SSH 和 SSL

密钥。将设备运出可信任环境边界时，请务必采取适当的 防范措施。 – 运输前，将 SSH 和 SSL

密钥替换为一次性密钥。 – 停用现有的 SSH 和 SSL 密钥。设备返厂后，为设备创建并设定新密钥。

使用 PKCS #12 格式的具有密码保护的证书。 使用密钥长度为 4096 位的证书。 将设备退回 Siemens

进行维修之前，请使用临时的一次性证书和密钥替换当前证书和密

钥，这些证书和密钥在设备返厂时可被销毁。

验证服务器和客户端上的证书和指纹，避免 “ 中间人 ” (MitM) 攻击。 物理/远程访问

仅可在受保护的网络区域内运行该设备。断开内部和外部网络时，攻击者无法从外部访 问内部数据。

应将该设备限制为仅允许可信任的人员进行物理访问。拥有设备可移动介质的恶意用户

可以提取证书、密钥等关键信息（用户密码通过哈希码保护）或对介质重新编程。

对串行控制台的访问控制错误应与对设备的物理访问控制措施相同。 强烈建议启用暴力破解 (BFA)

保护，以防止第三方未经授权访问设备。 有关详细信息，请参见 “ 补充文档 (页 8) ” 。

通过非安全网络进行通信时，需额外使用具有 VPN 功能的设备来加密和验证通信。

安全连接到服务器后（例如安全升级的情况）