西门子PLC授权总经销商 S7-1200 6ES7231-5PA30-0XB0 SB1231, 热电阻信号板模块

产品名称	西门子PLC授权总经销商 S7-1200 6ES7231-5PA30-0XB0 SB1231, 热电阻信号板模块
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:全国代理 S7-1200:现货 德国:全新
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授权总经销商 S7-1200 6ES7231-5PA30-0XB0 SB1231, 热电阻信号板模块

SIMATIC S7-1200，模拟输入， SB 1231RTD，1 AI RTD， PT 100 和 PT1000

PLC 到 PLC 通信（使用代码块中的通信指令）不受 CPU 中安全等级的限制。 表格 6-3 CPU 的安全级别
安全等级 访问限制 完全访问含故障 安全（无保护） 允许完全访问 F-CPU，没有密码保护。
完全访问（无保 护） 允许完全访问标准 CPU，没有密码保护。 读访问
无需输入密码即可对硬件配置和块进行读访问。可以将硬件配置和块上 传到编程设备。此外，具有 HMI 访问权和诊断数据访问权。可以显示离 线/在线比较结果，更改操作模式 (RUN/STOP) 以及设置时钟。
无法将块或硬件配置下载到 CPU 中。不能进行固件更新。 HMI 访问 仅允许 HMI 访问 除了可访问 HMI 面板，HMI 访问还允许使用大多数在线功能。有关详细 信息，请参见 TIA Portal Information System。
无访问权（完全 保护） 不输入密码无访问权。 只能看到标识数据，例如 “ 可访问设备 ”。 可以为 CPU 设置任何安全级别的紧急（临时）IP 地址 (页 823)。
密码区分大小写。要组态保护级别和密码，请按以下步骤操作： 1. 在 “ 设备组态 ” (Device configuration) 中，选择 CPU。 2. 在巡视窗口中，选择 “ 属性 ” (Properties) 选项卡。 3. 选择 “ 保护和安全 ” (Protection & Security) 属性以选择访问级别和输入密码。 将 S7-1200 CPU 升级为 V4.x 时， “ 更新密码加密 ” (Update password encryption) 按钮可升 级现有访问级别密码的存储格式。 当您将此组态下载至 CPU 时，用户将具有 HMI 访问权限，可以在无密码的情况下访问 HMI
功能。要读取数据或比较离线/在线代码块，用户必须输入 “ 读访问 ” (Read access) 的已组态 设备配置 6.8 防护与安全 S7-1200 可编程控制器 系统手册, V4.6 11/2022, A5E02486685-AP 161
密码或 “ 完全访问（无保护） ” (Full access (no protection)) 的密码。要写入数据，用户必须输入 “ 完全访问（无保护） ” 的已组态密码。要访问故障安全 CPU，用户必须输入 “ 完全访问含故障安全（无保护） ” (Full access incl. fail-safe (no protection)) 的密码。 警告 对受保护的 CPU

进行未授权访问 拥有 CPU 完全访问权限或完全访问权限（包括故障安全）的用户有权读写 PLC 变量。无论 CPU 访问级别是多少，Web 服务器用户都有权限读写 PLC 变量。未经授权访问 CPU 或将 PLC 变量更改为无效值可能会中断过程操作并可能导致死亡、严重人身伤害和/或财产损失。
授权用户可以执行操作模式更改、写入 PLC 数据以及进行固件更新。西门子建议您遵守以 下安全实践：
使用 STEP 7 中定义的强密码对 CPU 访问级别和 Web 服务器用户 ID (页 863) 进行密码保护。 仅使用 HTTPS 协议启用对 Web 服务器的访问。 不要扩展 Web 服务器 “ 所有人 ” (Everybody) 用户的默认*低权限。 对程序逻辑中的变量执行错误检查和范围检查，因为 Web 页面用户可将 PLC 变量更改为无 效值。 6.8.4 组态连接机制 6.8.4.1 设置远程伙伴的访问机制 要使用 PUT/GET 指令访问远程连接伙伴，用户还必须得到许可。 默认情况下， “ 允许使用 PUT/GET 通信进行访问 ” (Permit access with PUT/GET communication) 选项处于未启用状态。这时，只有需要对本地 CPU 和通信伙伴同时进行组态和编程的通信连接才能实现对 CPU 数据的读写访问。例如，可以通过 BSEND/BRCV 指令 进行访问。因此，本地 CPU 仅作为服务器的连接（也就是说，本地 CPU 中不存在带有通信伙伴的通信组态/编程）在 CPU 运行期间不可用，例如： 通过通信模块进行 PUT/GET、FETCH/WRITE 或 FTP 访问从其它 S7 CPU 进行 PUT/GET 访问 通过 PUT/GET 通信进行 HMI 访问 设备配置 6.8 防护与安全 S7-1200 可编程控制器 162 系统手册, V4.6 11/2022, A5E02486685-AP 如果您希望允许从客户端访问 CPU 数据，即您不希望限制 CPU 的通信服务，请按以下步骤 操作： 1. 将保护访问级别组态为除 “ 无访问（完全保护） ” (No access (complete protection)) 外的任意 级别。 2. 选择 “ 允许使用 PUT/GET 通信进行访问 ” (Permit access with PUT/GET communication) 复选框。
当您将此组态下载至 CPU 时，CPU 将允许与远程伙伴进行 PUT/GET 通信 6.8.4.2 启用安全 PG/PC 和 HMI 通信并创建证书 使用 CPU 设备组态中的 “ 连接机制 ” 来组态 CPU 的通信方式：仅接受安全通信还是同时接 受安全通信和传统通信。安全通信使用基于 TLS (Transport Layer Security) 1.3. 的 X.509 证 书。CPU 使用这些证书在 CPU 和客户端之间实现安全通信。客户端包括：TIA Portal SIMATIC Automation Tool HMI 选择 “ 仅允许安全 PG/PC 和 HMI 通信 ” (Permit only secure PG/PC and HMI communication) 以禁用传统 PG/PC 和 HMI 通信。
用户还可以创建自己的证书。单击 “ PLC 通信证书 ” 旁的 “ ... ” 为 CPU 添加新证书或选择现有证书。有关证书组态参数的详细信息，请参见 TIA Portal Information System 中的主题 “ 创建/ 更新证书 ” 。
设备组态的 “ 防护与安全 ” 中的组态部分提供有关安全选择的屏幕指南。这些部分还提供 TIA Portal Information System 中针对各组态任务和相关安全概念的主题链接。 传统通信
如果需要与不支持安全通信的设备进行通信，请取消选择 “ 仅允许安全 PG/PC 和 HMI 通信 ” (Permit only secure PG/PC and HMI communication)。通过进行此选择，PLC 便可使用安全通信或传统通信进行通信。 TIA Portal 默认采用***别的安全通信；但出于调试原因，可通过从 “ 在线 ” (Online) 菜单 中选择 “ 仅使用传统 PG/PC 通信 ” (Use only legacy PG/PC communication)，强制 TIA Portal 使用传统 PG/PC 通信。

对于 V4.x CPU，还可使用安全向导 (页 157)组态 PG/PC 和 HMI 通信。 警告 调试过程中的安全风险
调试期间，CPU 会提供一个自签名证书，您必须信任该证书才能建立连接。仅当编程设备和 CPU 位于受保护的网络上并且彼此直接连接时，才信任此证书。
在未受保护的环境中，攻击者可以修改这些证书并访问编程设备/HMI 和 CPU 之间的通信，例如，通过中间人攻击。
由于未受保护的通信环境造成的攻击可能会中断流程操作并导致死亡、严重的人身伤害或 财产损失。
6.8.5 外部装载存储器 也可以防止从内部装载存储器备份到外部装载存储器（SIMATIC 存储卡）。要防止从内部装 载存储器到外部装载存储器的复制操作，请按照以下步骤操作： 1. 在 STEP 7 中，从 CPU 设备组态的 “ 常规 ” (General) 属性中选择 “ 保护和安全 ” (Protection & Security)。 2. 在 “ 外部装载存储器 ” (External Load Memory) 部分，选择 “ 禁用从内部装载存储器到外部装载存储器的复制操作 ” (Disable copy from internal load memory to external load memory)。 有关该属性对 CPU 插入存储卡的影响，另请参见在 CPU 中插入存储卡 (页 118)主题。 6.8.6 专有技术保护
专有技术保护可防止程序中的一个或多个代码块（OB、FB、FC 或 DB）受到未经授权的访问。用户创建密码以限制对代码块的访问。密码保护会防止对代码块进行未授权的读取或修改。如果没有密码，只能读取有关代码块的以下信息： 块标题、块注释和块属性

传送参数（IN、OUT、IN_OUT、Return） 程序的调用结构
交叉引用中的全局变量（不带使用时的信息），但局部变量已隐藏
将块组态为 “ 专有技术 ” 保护时，只有在输入密码后才能访问块内的代码。
使用代码块的 “ 属性 ” (Properties) 任务卡组态该块的专有技术保护。打开代码块之后，从 “ 属性 ” (Properties) 中选择 “ 保护 ” (Protection)。 设备配置 6.8 防护与安全 S7-1200 可编程控制器 164 系统手册, V4.6 11/2022, A5E02486685-AP 1. 单击 “ 保护 ” (Protection) 按钮，显示 “ 专有 技术保护 ” (Know-how protection) 对话框。 2. 单击 “ 定义 ” (Define) 按钮输入密码。 3. 输入新密码并确认。 4. 单击 “ 确定 ” (OK) 后完成设置。 6.8.7 写保护
块的写保护功能可防止其意外更改。设置有写保护功能的块只能以 “ 只读 ” 方式打开，但块属性仍可编辑。 要设置代码块的写保护功能，请按以下步骤操作： 1. 打开代码块的 “ 属性 ” (Properties) 任务卡。 2. 打开代码块的属性之后，选择 “ 保护 ” (Protection)。 3. 在 “ 写保护 ” (Write protection) 区域中，选择 “ 定义密码 ” (Define password)。 4. 在 “ 定义保护 ” (Define protection) 对话框的 “ 新密码 ” (New password) 和 “ 确认密码 ” (Confirm password) 字段中输入密码。 5. 单击 “ 确定 ” (OK)，确认输入。 6. 选中 “ 写保护 ” (Write protection) 复选框。 7. 在 “ 访问保护 ” (Access protection) 对话框中，输入正确的密码。
在相应步骤后，下次打开该块时，写保护功能将启用并处于激活状态。 设备配置 6.8 防护与安全 S7-1200 可编程控制器 系统手册, V4.6 11/2022, A5E02486685-AP 165 6.8.8 复制保护
附加安全特性允许捆绑程序块，以用于特定存储卡或 CPU。该特性对于保护您的知识产权特别有用。当您将程序块与特定设备捆绑在一起时，就会将程序或代码块限制为仅用于特定存 储卡或 CPU。此特性允许用户通过电子方式（例如通过 Internet 或电子邮件）或发送存储卡的方式分配程序或代码块。复制保护可用于 OB (页 176)、FB (页 178) 和 FC (页 178)。 S71200 CPU 支持三种类型的块保护： 与 CPU 的序列号进行绑定 与存储卡的序列号进行绑定 与强制性密码动态绑定
使用代码块的 “ 属性 ” (Properties) 任务卡将该块捆绑到特定 CPU 或存储卡。 1. 打开代码块之后，选择 “ 保护 ” (Protection)。 2. 在 “ 复制保护 ” (Copy protection) 任务下的下拉列表中，选择要使用的复制保护的类型。 3. 对于与 CPU 或存储卡序列号的绑定，可以在下载时插入序列号，也可以输入存储卡或 CPU 的 序列号。 说明 序列号区分大小写。 对于与强制性密码的动态绑定，定义下载或复制块所必须使用的密码。 随后下载 (页 197)带有动态绑定的块时，必须输入可用于下载块的密码。请注意，复制保护 密码和专有技术保护 (页 164)密码是两个不同的密码。 设备配置 6.8 防护与安全 S7-1200 可编程控制器 166 系统手册, V4.6 11/2022, A5E02486685-AP 6.9 组态模块的参数
要组态模块的运行参数，请在设备视图中选择模块，并使用巡视窗口的 “ 属性 ” (Properties) 选项卡组态模块的参数。 组态信号模块 (SM) 或信号板 (SB) 使用与组态 CPU 的板载 I/O (页 151) 相同的步骤来组态 SM 或 SB 的 I/O。无法将信号模块输 入组态为上升沿检测 (页 74)、下降沿检测 (页 74)或脉冲捕捉 (页 154)。 组态通信接口（CM、CP 或 CB） 根据通信接口的类型组态网络参数。
设备配置 6.9 组态模块的参数 S7-1200 可编程控制器 系统手册, V4.6 11/2022, A5E02486685-AP