SIEMENS西门子 S-1FL2中惯量型电机 1FL2 203-2AG11-1SC0

产品名称	SIEMENS西门子 S-1FL2中惯量型电机 1FL2 203-2AG11-1SC0
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

安全统计选项 (IEC 60870-5-101/104) 安全统计数据 (IEC 60870-5-101/104)
下表包含符合 IEC/TS 60870-5-7 和 IEC/TS 62351-5 的安全统计选项，可针对不同遥控连接
分段进行组态。 选项 (IEC) 可在 IEC 连接的 “ 第 1 路径选项 ” (Options 1st Path)/ “ 第 2
路径选项 ” (Options 2nd Path) 参数 组中找到以下参数。 调用间隔
以下参数定义了主站对站的特殊调用间隔 (cause of transmission 20 - 41)。
所有参数都被组态为 “ 基本轮询间隔 ” 的倍数（请参见主站）。 一般请求间隔
定义应答主站的一般请求的时间间隔。 组请求间隔 定义应答相应的主站组请求的时间间隔。
计数器的一般请求间隔 定义应答主站计数器的一般请求的时间间隔。 计数器的组请求间隔
定义应答相应的主站计数器的组请求的时间间隔。
用户可以定义关于是否应答一般请求的设置，以及对数据点组态中每个单独数据点的组请求 分配。 带 3
个服务器的冗余 DNP3 主站组 与三个服务器的 DNP3 连接
通过连接到冗余控制中心，一个通信模块最多可以同时与主站建立 2 个连接。
在特定连接组态的情况下，如果冗余组的两个连接之一发生故障，则作为分站的模块可以与
第三个服务器建立连接。组态站模块 取消激活 “ IP 地址检查 ” (IP address check) 参数 –
对于站的通信模块，打开参数组 “ 以太网接口 > gaoji选项 > DNP3 站设置 ” (Ethernet interface > Advanced options > Settings DNP3 station)。 – 将 “ IP 地址检查 ” (IP address check) 选项设置为 “ 不检查 IP
地址 ” (Do not check IP address)。 在此设置中，不会检查通信伙伴的 IP
地址。这可确保网络中任何使用主站的 DNP3 站地 址组态的站都可以连接到站模块，而无论其 IP
地址如何。 创建连接 1. 通过通信模块和网络创建站，连接各站并组态组件。
请勿为三个主站创建任何站。在 STEP 7 中，这些主站在遥控连接编辑器中组态为 “ 第三方设 备 ” (Third-party device)。 2. 在 “ 网络数据 ” (Network data) 任务卡中与 CP 创建两个 DNP3 连接。 3. 在 “ 网络数据 > TeleControl > DNP3 ” (Network data > TeleControl > DNP3) 任务卡中与站模块 创建两个 DNP3 连接。
两个连接段几乎完全相同，但是 “ 最终接口（冗余） ” (End interface (red.)) 参数的组态有所 不同：

两个连接段具有以下组态： Section_1 – 起点 (Starting point)：通信模块 (outstation) – “ 起始接口 ”(Start interface)：模块的以太网接口 – “ 起始接口（冗余） ”(Start interface (red.))：模块的以太网接口 – 端点 (End point)：第三方设备 – “ 最终接口 ”(End interface)：主站 1 接口的 IP 地址 – “ 最终接口（冗余） ”(End interface (red.))：主站 2 接口的 IP 地址 Section_2 – 起点 (Starting point)：通信模块 (outstation) – “ 起始接口 ”(Start interface)：模块的以太网接口 – “ 起始接口（冗余） ”(Start interface (red.))：模块的以太网接口 – 端点 (End point)：第三方设备 – “ 最终接口 ”(End interface)：主站 1 接口的 IP 地址 – “ 最终接口（冗余） ”(End interface (red.))：主站 3 接口的 IP 地址 下图显示了三个冗余主站的连接表示例。

启用这些选项后，通信模块（站）将安全统计事件发送给主模块，以进行进一步评估。基于这些事件的频率可得出关于系统可能存在漏洞或遭受攻击的结论。 安全统计选项 如果使用 Secure Authentication，则站会保留不同值的统计数据。 事件通过 ASDU 类型"Information 41" (integrated total for the statistic)传送。 下表列出了模块支持的符合 IEC/TS 62351-5 标准的统计参数。 阈值 (Threshold) 可以为每个统计值组态一个阈值。如果超出该阈值，则会触发向伙伴传送事件的行为。 值范围是 0...65535。 该值设置为 0（零）时，将禁用此功能。如果该值有问题，则不会传送相应统计数据。CPU 与遥控模块之间的通信 CP：通过背板总线进行通信 如果 CPU 和遥控 CP 位于同一机架中，则它们之间的通信通过背板总线进行。CPU 会自动分 配给遥控 CP。TIM 1531 IRC：通过以太网与 CPU 进行 TLS 通信 TIM 1531 IRC 未插入 CPU 的机架中，而是插入单独的机架中。与 CPU 的连接通过以太网进行， 并通过 TLS 针对所有可用的遥控协议使用安全通信。 对于通过 TLS 进行的通信，需要使用新创建的 CPU 证书并将其指定给 “ 用户数 ” (Subscriber numbers) 参数组中的 TIM。为 CPU 创建证书并将 TIM 分配给 CPU 时，会自动输入证书。 创建 CPU 证书并指定 CPU 要求 要创建和分配证书，必须满足以下要求： 作为 STEP 7 项目用户，至少拥有 “ NET Administrator ” 角色的权限。 更多相关信息，请参见 “ 安全设置 > 用户和角色 > 已分配角色 ” (Security settings > Users and roles > Assigned roles)。 设备具有所需的最低固件版本，请参见上文。 CPU 的组态数据受到保护。 更多相关信息，请参见 “ 保护与安全 > 机密 PLC 组态数据保护 ” (Protection & Security > Protection of confidential PLC configuration data) 要将本地 CPU 指定给 TIM 1531 IRC，必须满足以下要求： CPU 与 TIM 1531 IRC 已连接网络。 在 “ 通信类型 ” (Communication types) 下为 TIM 启用了所需的遥控协议。 SIMATIC NET 设备的证书 SIMATIC NET 通信模块通常使用全局证书管理器。相关信息，请参见项目导航中 “ 安全设置 > 安全功能 ” (Security settings > Security features)。 创建 CPU 证书 首先，需要为 CPU 创建一个由系统生成的证书（STEP 7 项目的全局证书管理器）。CPU 本 地创建的证书不能用于通信。 将 CPU 分配给 TIM（见下文）后，新创建 CPU 证书的 ID 会自动输入到以下位置： TIM 的 “ 用户编号 ” (Subscriber numbers) 对话框中 在 TIM 的证书管理器中作为合作伙伴证书请按以下步骤创建 CPU 证书： 1. 为 CPU 选择参数组 “ 保护与安全 > 证书管理器 > 全局安全设置 ” (Protection & Security > Certificate manager > Global security settings)。 2. 启用 “ 使用证书管理器的全局安全设置 ” (Use global security settings for the certificate manager) 选项。 注意： 启用该选项后，将删除现有证书。 3. 转至 “ 保护与安全 > 连接机制 > 与 TIA Portal 和 HMI 通信 ” (Protection & Security > Connection mechanisms > Communication to TIA Portal and HMI) 4. 在 “ PLC 通信证书 ” (PLC communication certificate) 行中，右键单击相应图标以打开下拉列表。 5. 在打开的下拉列表中单击 “ 添加 ” (Add)。 将打开包含以下选项的 “ 创建证书 ” (Create certificate) 对话框，其中包括： – 用途 (Usage)：TLS Client / Server – 认证机构 (CA) (Certificate authority (CA))由认证机构签发 (Signed by certification authority) – 主题的公用名 (Common name of subject)：所选 CPU 的名称 – 加密方法 (Encryption method)： EC – 散列算法 (Hash algorithm)： sha256 必要时，可以在 “ 主题备用名称 (SAN) ” (Subject Alternative Name (SAN)) 下为 CPU 添加其它 地址类型。 6. 保留设置并单击 “ 确定 ” (OK)。 新创建的 TLS 证书与 CPU 的 “ TlsServer ” 服务一起显示在设备证书表中。 7. 在项目导航中打开全局证书管理器： “ 安全设置 > 安全功能 > 证书管理器 > 设备证书 ” (Security settings > Security features > Certificate manager > Device certificates) 8. 选择新创建的 CPU 证书（ID 见上文），然后打开 “ 分配 ” (Assign) 快捷菜单。 9. 在列表中，选择应分配 CPU 的 TIM。 10.在（ “ 未分配 ” (Not assigned)）单元格的 “ 使用方式 ” (Used as) 行中，选择 “ 受信任的证 书 ” (Trusted certificate) 选项并单击绿色复选标记。 11.单击 “ 确定 ” (OK)

关闭对话框。 将 CPU 分配给 TIM 1531 IRC 1. 对于要与 CPU 通信的 TIM，打开“ 用户数 ”(Subscriber numbers) 参数组。 2. 在“ 已分配的 CPU ”(Assigned CPU) 行中，右键单击相应图标以打开下拉列表。 将打开已连接网络的 CPU 的列表。 3. 选择要分配给 TIM 的 CPU，然后单击其下方的绿色复选标记。 CPU 的名称即显示在“ 已分配 CPU ”(Assigned CPU) 行中。 同时，之前为 CPU 创建的证书 ID 会自动显示在“ 通信证书 ”(Communication certificate)行中。 更多组态
然后将其它站组态为通信伙伴和相应的遥控连接。