SIEMENS西门子数控系统授权总经销商 6ES7193-6BP00-0BA0

产品名称	SIEMENS西门子数控系统授权总经销商 6ES7193-6BP00-0BA0
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:代理销售商 ET200:全新原装 德国:正品现货
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

用户、角色和功能权限 - 新方法的详细信息在 TIA Portal 的先前版本中，用户和角色也在“ 安全设置 > 用户和角色 ”(Security settings >Users and roles) 下进行管理。除了现有的用户管理选项（例如 HMI 设备的用户管理选项）之外，自 TIA Portal V19 起还可以在此编辑器中管理所有 CPU 功能权限。CPU 功能权限在运行系统中有效，因此，这些权限位于用户和角色编辑器的“ 运行系统权限 ”(Runtime rights) 选项卡中。对于项目中的每个 CPU，都有一个专门区域用于选择所有 CPU功能权限 - 根据 CPU 服务，例如 PG/HMI 通信（工程组态访问、访问级别），Web 服务器和OPC UA 划分为不同的部分。除了项目的用户管理，CPU 的属性中还提供 Web 服务器和 OPC UA 服务器的用户管理选项（固件版本不超过 V3.0 的 CPU 支持静态用户管理）： OPC UA 服务器的用户（身份验证） Web 服务器的用户（身份验证和访问控制）自 TIA Portal V19 和 CPU 固件版本 V3.1 起，这些额外的用户管理选项已集成到项目树的本地用户管理中。188分布式 I/O 系统系统手册, 11/2023, A5E03576855-AN保护11.3 本地用户管理本地用户管理和访问控制简介对于固件版本 V3.0 及以下的 CPU，用户在各个服务“ Web 服务器 ”、“ OPC UA ”等的相应 CPU 属性下进行管理。Web 服务器用户在“ Web 服务器 ”(Web server) 区域中进行管理，OPC UA 用户在“ OPC UA ”区域中进行管理。要使用访问级别限制 PG/HMI 对 CPU 的访问，请为相应级别分配密码。例如，通过此方法，HMI 访问可以不受限制，但写访问需要视密码的已知情况而定。各访问级别的密码在 CPU 属性的“ 保护和安全 ”(Protection & Security) 区域进行分配。因此，访问保护始终适用于具有相应密码的组，而不适用于个人用户。在 TIA Portal V19 版本中引入本地用户管理和访问控制后，可以使用 TIA Portal 的项目树中的“ 安全设置 > 用户和角色 ”(Security settings > Users and roles) 区域管理所有用户及其角色和CPU 的功能权限。这同样适用于工程组态/HMI 访问的访问保护，自 TIA Portal 版本 V19 起，该功能不再默认通过密码保护的访问级别实现，而是通过用户管理实现。有关新访问保护的更多信息，请访问此处 (页 192)。例如，正如引入的工程组态权限一样，使用角色分配来组合单个功能权限。在后续步骤中，可将角

色分配给各个用户。在“ 已分配的权限 ”(Assigned rights)
选项卡中列出了通过角色分配给用户的所有功能权限，以及该用户可对相应 CPU 执行的功能权限。CPU 的可用和激活功能权限示例如下图所示。必须至少有一个用户对 CPU
具有完全访问权。否则，将无法编译组态。为此，必须创建对 CPU 具有完全访问权限的角色。图 11-1 为角色分配 CPU 功能权限下图显示了将具有完全访问权限的角色分配给用户（“ Admin ”）。图 11-2 向用户分配角色189保护11.3 本地用户管理分布式 I/O 系统系统手册, 11/2023, A5E03576855-AN要求CPU
参数分配：要使用用户、角色和 CPU 功能权限，必须在“ 保护和安全 > 访问控制 ”(Protection & Security > Access control) 区域中选择“ 启用访问控制 ”(Enable access
control)选项。本地用户管理不需要项目保护。默认特性默认为访问控制选择“ 启用访问控制 ”(Enable access control) 选项。可以使用分配的密码以及角色和功能权限对用户进行组态。下载到设备可在 CPU 处于 STOP 和 RUN 模式时下载对本地用户管理和访问控制组态的更改。运行系统超时可在“ 安全设置 > 用户和角色 ”(Security Settings > Users and Roles) 中设置角色和用户的运行系统超时属性。对于 ET 200SP CPU，多种服务可采用这些设置，如下所示： 通过 Web API，可创建采用运行系统超时设置的 Web 页面或应用。标准 Web 页面不采用运行系统超时设置，并使用默认值。 其它服务（PG/HMI 通信和 OPC UA 服务器）不使用运行系统超时；已登录用户在设定时间后并不会退出。11.3.2
本地用户管理和访问控制的优势下文将介绍新的 CPU
本地用户管理的优势以及与之相关的更改。快速激活/禁用本地用户管理用户管理选项位于“ 保护和安全 > 访问控制 ”(Protection & Security > Access control) 区域中： 访问控制禁用：除了用于在线传送证书的 GDS 推送功能外，每个用户都可以完全访问所有功能。危险禁用访问控制功能可能会发生未经授权的访问，从而造成人身伤害和财产损失。例如，在调试期间，仅在受保护的环境中使用此设置。
访问控制启用：已组态的用户及其分配的角色和相关功能在下载组态后生效。PG/HMI
访问的访问保护，现在采用用户身份验证对于固件版本 <V3.1 的
CPU，可分配访问级别的密码，而对于最新版本的
CPU，可为用户组态相应的功能权限。这意味着可以采用与 OPC UA 和 Web 服务器访问相同的方式对 PG/HMI 访问进行身份验证。190分布式 I/O 系统系统手册, 11/2023, A5E03576855-AN保护11.3
本地用户管理集中管理一切无论在 CPU 中组态用户、角色和权限时使用何种服务：在同一个位置管理数据。无论是管理项目的工程组态权限还是项目中各个 CPU
的本地运行系统权限，所有用户均可在用户和角色编辑器的项目树中找到。强大的密码功能
创建密码时对复杂性规则的遵守情况：在创建密码阶段，就已可以在 TIA Portal
中检查复杂性规则的遵守情况，例如有关密码长度、大写/小写字母的规则（项目树的“ 安全设置 > 设置 ”(Security settings > Settings) 区域）。在下载用户管理时，复杂性规则也保存在 CPU
中。在线修改密码时，由 CPU
识别并应用这些规则。这可防止用户覆盖组态工程师设置的复杂性规则并分配不安全的密码。
可以设置密码的有效期：为了防止用户继续长期使用已泄露的密码访问 CPU，可分配密码的有效期。然后在登录时提示有效期到期之前剩余的有效时间，以便用户可以及时更改密码。运行期间加载用户管理自固件版本 V3.1 起，可在处于 STOP 和 RUN
系统状态时下载某些与安全相关的组态数据。这意味着下载硬件配置并不一定会导致 CPU 进入 STOP 状态。可在处于 STOP 和 RUN 系统状态时下载以下更改（下载到设备 > 硬件配置）：
扩展/更改本地用户管理 添加/修改 TIA Portal 组态的证书 更改 Syslog
组态如果对硬件配置进行其它更改（例如，添加模块、重新分配参数等），则 CPU
将在下载组态之前自动提示用户，CPU 将进入 STOP
状态。因此，如果只是将修改过角色/功能权限的用户下载到 CPU，并不会导致 CPU 进入 STOP
状态。下载预览对话框包含一个安全区域，可以在其中定义 CPU 如何处理自上次下载操作以来（而不是首次下载时）更改的用户数据。允许保留对用户数据的更改（例如，运行期间的密码更改）。将设备作为新站下载 - 包含用户数据如果将先前组态的 CPU
下载到新项目中，由于没有原始项目，用户数据也将下载到此新项目中，并可用于进一步编辑 CPU 设置。191保护11.3 本地用户管理分布式 I/O 系统系统手册, 11/2023,
A5E03576855-AN在操作期间更改密码通过 Web 服务器 API 编写的应用程序，所有用户均可在运行系统中更改密码，前提条件是正确输入了原始密码，并且新密码符合组态的密码策略。要求：已启用 CPU 访问控制。用户可随时修改密码，不受密码已过期的影响。如果密码已过期，用户必须更改密码。密码过期后无法登录。使用的 API 方法： Api.ChangePassword Api.GetPasswordPolicy有关 API

方法的更多信息，请参见《S7-1500 CPU 的 Web 服务器》功能手册。说明运行期间更改的密码优先于下载的密码如果在运行期间更改了密码并在随后下载了项目，则在运行期间分配的密码优先于项目中设置的密码（默认设置）。如果要通过下载项目来覆盖在运行期间更改的密码，则必须选择“ 下载所有用户管理数据（复位为项目数据） ”(Load all user administration data (reset to project data))
选项。在这种情况下，运行期间更改的所有密码都将丢失。

从访问级别到用户功能权限下文将介绍如何使用新的本地用户管理来实现 CPU
访问保护。作为功能权限的访问级别对于固件版本不超过 V3.0 的 ET 200SP
CPU，仅可通过密码控制访问；而对于固件版本自V3.1 起的 CPU，可创建具有必要功能权限的相应用户和角色进行访问控制。访问级别和相关功能权限之间的分配基于已知的访问级别： 要拥有完全访问权限，用户必须具有功能权限“ 完全访问 ”的角色。只有当至少一个用户具有“ 完全访问 ”或“ 完全访问（故障安全） ”功能权限时，才能编译和下载 CPU 组态。
要拥有只读访问权限，用户必须具有功能权限“ 只读访问 ”的角色。 要拥有 HMI
访问权限，用户必须具有功能权限“ HMI
访问 ”的角色。如果用户不具备这些功能权限，则该用户也没有 CPU
的访问权限。访问级别的层级结构以及相应的功能权限保持不变：
具有完全访问权限的用户仍具有“ 只读访问 ”和“ HMI 访问 ”功能权限。
具有只读访问权限的用户仍具有“ HMI 访问 ”功能权限。说明“ ENDIS_PW ”指令的兼容性“ ENDIS_PW ”指令仅可禁用或启用防护等级的密码。“ ENDIS_PW ”指令对分配的用户或角色权限没有影响。

继续使用访问级别尽管新的本地用户管理通过各个用户的相应功能权限取代了常见的访问保护，但仍可选择继续使用这一常见的访问保护功能。例如，对于仅支持访问级别并且无法使用新用户管理的 HMI设备而言，仍需要使用访问保护功能。如果需要组态访问级别，以允许在没有分配用户和密码的情况下访问 HMI 设备，可在 CPU 属性中选择“ 通过访问级别使用传统访问控制 ”(Use legacy access control via access levels) 选项。说明OPC UA 和 Web
服务器的用户无论采用哪种访问保护方式，必须在项目树中（“ 安全设置 > 用户和角色 ”(Security settings >Users and roles) 区域）组态 Web 服务器和 OPC UA
服务器的用户。继续使用访问级别的限制使用“ 传统访问控制 ”(Legacy access control) 选项时，不能直接在访问级别设置表中选择访问级别。只能通过以下一种方式为新的本地用户管理设置此选项：使用“ 匿名 ”(Anonymous) 用户的访问保护功能权限。系统默认在项目中创建本地“ 匿名 ”(Anonymous)
用户。借助此用户，可以在没有用户名和密码的情况下进行登录时，定义项目中 CPU 的特性。出于安全考虑，匿名用户已禁用，如需使用必须先进行激活。在访问级别设置区域中通过链接跳转到编辑器，以进行所需的“ 匿名 ”(Anonymous) 用户设置。示例： 如果“ 匿名 ”(Anonymous)
用户被禁用或者“ 匿名 ”(Anonymous) 用户虽然激活但没有分配任何功能权限，则没有用户名和密码任何人都不能登录（对应于访问级别“ 不能访问（完全保护） ”(No access (complete protection))）。
如果“ 匿名 ”(Anonymous) 用户被激活并且 CPU 的“ 完全访问 ”(Full access)
功能权限通过相应的角色分配给该用户，则此设置的结果为“ 无保护 ”(No protection)。通过在 CPU 属性的“ 保护和安全 ”(Protection & Security) 区域中设置“ 不能访问保护 ”(No access
protection)，也可以达到此目的。操作步骤要激活“ 传统访问控制 ”(Legacy access control)
并设置所需的访问级别，请按以下步骤进行操作：1. 在 CPU 属性中，转到“ 保护和安全 >
访问控制 ”(Protection & Security > Access control)。2. 选择“ 启用访问控制 ”(Enable access control)
选项，并选中“ 通过访问级别使用传统访问控制 ”(Use legacy access control via access levels)
复选框。不能在此设置中使用访问级别选择。使用 CPU 的“ 匿名 ”(Anonymous)
用户设置访问级别。默认情况下，“ 匿名 ”(Anonymous)
用户处于停用状态。这意味着，没有密码的用户的访问级别为“ 不能访问（完全保护） ”(No access (complete protection))（默认设置）。3. 在项目树中，转至“ 安全设置 > 用户和角色 ”(Security Settings > Users and roles)。4. 如果要设置“ 不能访问（完全保护） ”(No access (complete protection))
之外的访问级别，请激活“ 匿名 ”(Anonymous) 用户。可为激活的“ 匿名 ”(Anonymous)
用户分配一个具有功能权限的角色，该角色无需输入密码即可访问 CPU。5. CPU
的功能权限不能直接分配给用户。必须先创建角色：因此，切换到“ 角色 ”(Roles)
选项卡并添加新角色。分配一个有意义的名称，例如“ PLC1 只读访问角色 ”(PLC1-Read-Access-

Role)。如果将此角色分配给某个用户，则该用户在运行期间将具有 PLC1 的只读访问权限。6. 将访问 CPU “ PLC1 ” 所需的功能权限分配给角色 “ PLC1 只读访问角色 ” (PLC1-Read-Access-Role)，在本例中为 “ 只读访问 ” (Read access)。7. 切换到 “ 用户 ” (Users) 选项卡，将 “ PLC1 只读访问角色 ” (PLC1-Read-Access-Role) 角色分配给激活的 “ 匿名 ” (Anonymous) 用户。结果：“ 匿名 ” (Anonymous) 用户具有 PLC1 的只读访问权限。这意味着，项目中CPU “ PLC1 ” 的访问级别表被预设为 “ 只读访问 ” (Read access)（无法更改），未登录的用户只有只读访问权限。对于完全访问或完全访问（故障安全），必须在表中组态完全访问密码，以实现访问保护。对于在运行期间执行操作需要获取 CPU 完全访问的用户（例如，将项目下载到 CPU上），必须使用此密码登录后才能执行此操作。提示为了便于识别用户权限，相应角色应使用有意义的名称。为整个项目创建用户和角色；必须为项目中的每个 CPU 单独选择角色的功能权限。描述性名称允许用户立即识别授予只读访问权限的 CPU 和未授予访问权限的 CPU（完全保护）。