SIEMENS

SIMATIC

S7-1500
安全性

入门指南

03/2013

A5E03982402-01

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

⚠危险
表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

⚠警告
表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

⚠小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。 由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用 Siemens 产品

请注意下列说明：

⚠警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号 ® 的都是西门子股份有限公司的注册商标。本印刷品中的其他符号可能是一些其他商标。若第三方出于自身目的使用这些商标，将侵害其所有者的权利。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
德国

A5E03982402-01
℗ 06/2013 本公司保留技术更改的权利

目录

1 CPU 保护功能的概述

1

简介

本章描述了下列用于防止对 S7-1500 自动化系统进行未经授权的访问的功能：

- 访问保护
- 专有技术保护
- 防拷贝保护
- 通过锁定 CPU 进行保护

保护 CPU 的其它措施

下列措施进一步防止了从外部源和网络对 S7-1500 CPU 的功能和数据进行未经授权的访问。

- 禁用 Web 服务器
- 禁用通过 NTP 服务器的时间同步
- 禁用 PUT/GET 通信

使用 Web 服务器时，通过在用户管理中设置特定用户的密码保护访问权，可防止对 S7-1500 自动化系统进行未经授权的访问。

2 使用显示屏组态其它访问保护

简介

在 S7-1500 的显示屏上，可防止对受密码保护的 CPU 进行访问（本地锁定）。 仅当操作模式开关处于 RUN 位置时，此访问锁定才生效。
是否应用访问锁定与密码保护无关。即，如果某人通过连接的编程设备访问了 CPU 并且已输入正确的密码，同样会阻止该用户访问 CPU。
可以分别为显示屏上的每个访问级别设置访问阻止，这样就可以在本地允许读取访问，但是不允许写入访问。

操作步骤

如果在 STEP 7 中组态了使用密码的访问级别，则可使用显示屏来阻止访问。

按照以下操作在显示屏上设置 S7-1500 CPU 的本地访问保护：

1. 在显示屏上，选择“设置 > 保护”(Settings > Protection) 菜单。
2. 单击“确定”(OK) 进行确认选择，并组态每种访问级别中是否允许在 RUN 模式选择开关下访问：

   允许 (Allow)： 如果输入 STEP 7 中指定的密码，则可以访问 CPU。

   在 RUN 模式下禁用：当操作模式开关位于 RUN 位置时，即便其他用户知道该访问级别的权限密码，也无法登录该 CPU。 在 STOP 模式下，可通过输入密码进行访问。

显示屏访问保护

可以在 STEP 7 中的 CPU 属性中为显示屏组态密码，这样本地访问保护就可由本地密码进行保护。

3 专有技术保护

可以使用专有技术保护来保护程序中一个或多个 OB、FB、FC 类型的块以及全局数据块，防止受未经授权的访问。 可以输入密码限制对块的访问。 密码保护可防止在未经授权的情况下读取或更改块。

如果没有密码，则只能读取有关块的以下数据：

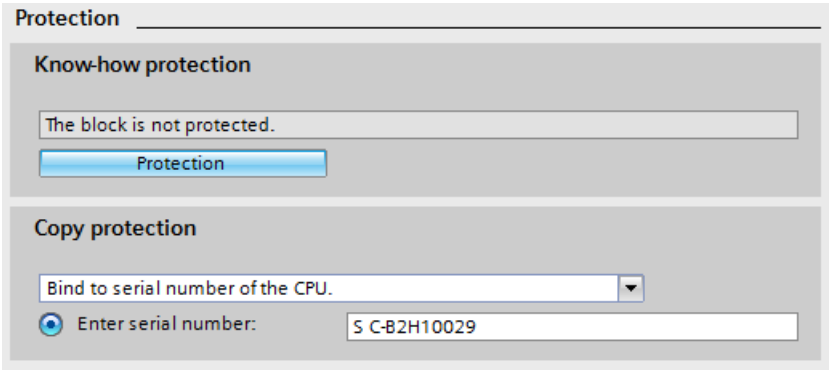
- 块标题、注释和块属性
- 块参数（INPUT、OUTPUT、IN、OUT、RETURN）
- 程序调用结构
- 不带使用点信息的全局变量

对于受到专有技术保护的块，可执行以下进一步操作：

- 复制和删除
- 在程序中调用
- 在线/离线比较
- 加载

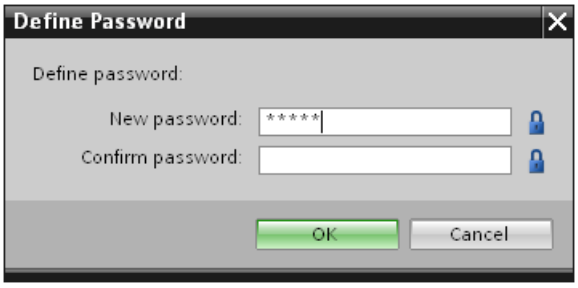
设置块的专有技术保护

1. 打开相应块的属性。
2. 请在“常规”(General) 下选择“保护”(Protection) 选项。



3. 单击“保护”(Protection) 按钮，显示“专有技术保护”(Know-how protection) 对话框。

4. 单击“定义”(Define) 按钮，打开“定义密码”(Define password) 对话框。



5. 在“新密码”(New password) 域中输入新密码。 在“确认密码”(Confirm password) 域中输入相同的密码。
6. 单击“确定”(OK)，确认输入。
7. 单击“确定”(OK)，关闭“专有技术保护”(Know-how protection) 对话框。

结果： 所选块将受到专有技术保护。 在项目树中，受专有技术保护的块将标记为一个锁形标识。 输入的密码将应用于所选的所有块。

打开受到专有技术保护的块

1. 双击块，将打开“访问保护”(Access protection) 对话框。
2. 输入受专有技术保护块的密码。
3. 单击“确定”(OK)，确认输入。

结果： 将打开受专有技术保护的块。

打开该块之后，只要该块或 TIA Portal 打开，就可以编辑该块的程序代码和块接口。 下次打开块时，必须重新输入密码。 如果使用“取消”(Cancel) 按钮关闭“访问保护”(Access protection) 对话框，则块虽然可以打开，但不显示块代码也不能进行编辑。

如果复制块或将其添加到库中，不会删除块的专业技术保护。 这些副本块同样也受专有技术保护。

删除块的专有技术保护

1. 选择要删除专有技术保护的块。 不能在程序编辑器中打开受保护的块。
2. 在“编辑”（Edit）菜单中，选择“专有技术保护”（Know-how protection）命令以打开“专有技术保护”（Know-how protection）对话框。
3. 禁用复选框“隐藏代码（专有技术保护）”(Hide code (know-how protection))。

4. 输入密码。

5. 单击“确定”(OK)，确认输入。

结果： 将删除所选块的专有技术保护。

4 防拷贝保护

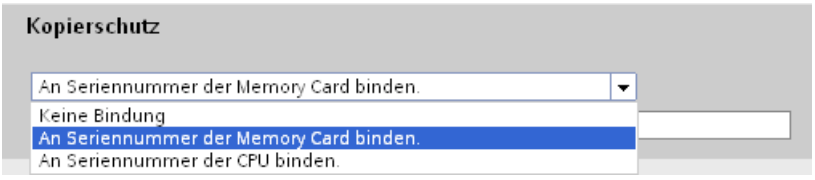
防拷贝保护则需将程序或块与一个特定的 SIMATIC 存储卡或 CPU 进行绑定。 通过链接 SIMATIC 存储卡或 CPU 的序列号，该程序或块只能与 SIMATIC 存储卡或 CPU 一起使用。 使用这一功能，可通过电子方式（例如，通过电子邮件）或通过发送存储器模块的方式来发送程序或块。

为块设置此类防拷贝保护时，还为其分配了专有技术保护。 未设置专有技术保护时，任何人都可以复位该防拷贝保护。 然而当该块已设置为受专有技术保护时，则首先应该将防拷贝保护设置为只读。

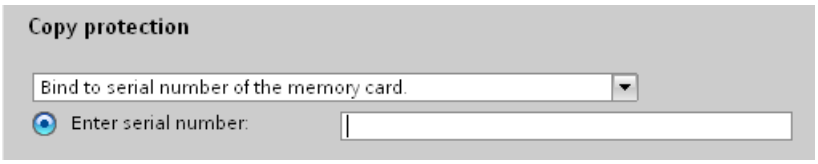
设置防拷贝保护

1. 打开相应块的属性。
2. 请在“常规”(General) 下选择“保护”(Protection) 选项。

3. 在“防拷贝保护”（Copy protection）区域中，从下拉列表中选择“绑定 CPU 的序列号”（Bind to serial number of the CPU）条目或“绑定存储卡的序列号”（Bind to serial number of the memory card）条目。



4. 输入 CPU 或 SIMATIC 存储卡的序列号。



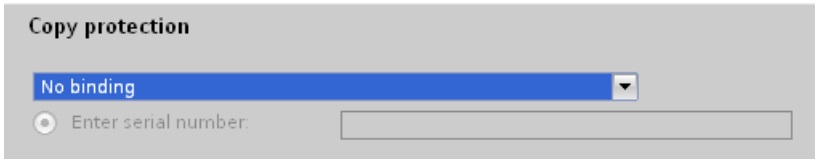
5. 现在，可以在“专有技术保护”(Know-how protection) 区域中设置块的专有技术保护。

说明

如果将受防拷贝保护的块下载到与特定序列号不匹配的设备中，则将拒绝执行整个下载操作。 这意味着，也不会下载不带防拷贝保护的块。

取消防拷贝保护

1. 取消现有专有技术保护。
2. 打开相应块的属性。
3. 请在“常规”(General) 下选择“保护”(Protection) 选项。
4. 在“防拷贝保护”（Copy protection）区域中，从下拉列表中选择“不帮定”（No binding）条目。

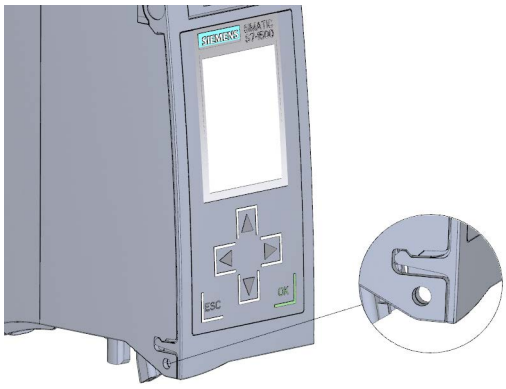


5 通过锁定 CPU 进行保护

可以使用坚固的前盖板，防止 CPU 免到受未经授权的访问。

通过 CU 外盖上的锁具，可进行如下选择：

- 加盖印章
- 使用锁具锁定前盖板（锁孔直径：3 mm）



6 组态 CPU 的访问保护

简介

CPU 中共有四种访问级别，用于限制对特定功能的访问。

设置 CPU 的访问等级和密码后，则需输入密码才能访问功能和存储区。 将在 CPU 的对象属性中指定各种访问级别以及相关的密码条目。

CPU 的访问级别

访问级别	访问限制
完全访问权（无保护）	所有用户都可以对硬件配置和块进行读取和更改操作。
读访问权	在这一级访问中，可以不输入密码对硬件配置和块进行只读访问。即，可将硬件配置和块加载到编程设备中。 还可以进行 HMI 访问和诊断数据访问。 但不输入密码，无法将任何块或硬件配置加载到 CPU 中。 此外，如果没有密码，也**无法**进行以下操作： 写入的功能测试、更改操作模式 (RUN/STOP) 以及固件更新（在线）。
HMI 访问权	在这一级访问中，不输入密码只能访问 HMI 和诊断数据。 如果不输入密码，既不能将块和硬件配置加载到 CPU 中，也无法从 CPU 中将块和硬件配置加载到编程设备中。 此外，如果没有密码，也**无法**进行以下操作： 写入的功能测试、更改操作模式 (RUN/STOP) 以及固件更新（在线）。
无访问权（完全保护）	对 CPU 进行完全保护时，无法对硬件配置和块进行读写访问。 同样无法进行 HMI 访问。 PUT/GET 通信的服务器功能在该访问级别中被禁用（无法更改）。 必须通过密码验证，才能提供 CPU 的完全访问权。

无论是哪一种访问级别，都可以无限制地访问某些功能而无需输入密码。例如，使用“可访问的设备”(Accessible devices) 功能进行识别。

CPU 的默认设置为“无限制”(No restriction) 和“无密码保护”(No password protection)。 要保护对 CPU 的访问，必须编辑 CPU 的属性并设置密码。

除非禁用了 PUT/GET 通信，否则 CPU 之间的通信（通过块中的通信功能）不受 CPU 的保护等级限制。

权限密码条目允许访问对应级别中允许的所有功能。

说明

组态一个访问级别并不能取代专有技术保护

通过限制下载权限，组态访问级别可防止对 CPU 进行未经授权的更改。 但不会对 SIMATIC 存储卡上的块设置受读写保护。 而使用专有技术保护则可以保护 SIMATIC 存储卡上的代码块。

对过程进行访问级别参数设置

请按以下步骤组态 S7-1500 CPU 的访问级别：

1. 在巡视窗口中，打开 S7-1500 CPU 的属性。
2. 在区域导航中打开“保护”(Protection) 条目。

   将在巡视窗口中显示一张列有各种访问级别的表格。

Protection level	Access			Access permission	
Protection	HMI	Read	Write	Password	Confirmation
Full access (no protection)	✓	✓	✓		
Read access	✓	✓			
HMI access	✓				
No access (complete protection)					

3. 激活表格第一列中所需的保护等级。 此列中相应访问级别右侧的绿色复选标记将指示如不输入密码仍可执行的操作。
4. 在“密码”(Password) 列中，为所选访问级别指定一个密码。 在“确认”(Confirmation) 列中，再次所选输入密码以免输入错误。

   确保密码足够安全，即，不要按照机器可识别的模式来设置密码。

   必须在第 1 行中输入密码（“完全访问权”访问级别）。 知道该密码的用户就可以不受限制地访问 CPU，而无需考虑所选保护等级。
5. 如果所选访问级别允许的话，可以根据需要将额外的密码分配到其它访问级别。
6. 将硬件配置下载到 CPU，以使访问级别生效。

操作期间受密码保护的 CPU 的行为

CPU 保护在将设置下载到 CPU 之后生效。

在执行在线功能之前，需检查所需的权限，必要时提示用户输入密码。 在任何时刻，只能在一个 PG/PC 执行受密码保护的功能。 其它 PG/PC 无法登录。

保护数据的访问授权在在线连接时间内有效，或在通过“在线 > 删除访问权限”(Online > Delete access rights) 手动取消访问授权之前保持有效。

在 RUN 模式下，对受密码保护的 CPU 进行的访问仅限于在本地显示屏中进行，同时也不能进行使用密码的访问。

7 组态 HMI 连接保护

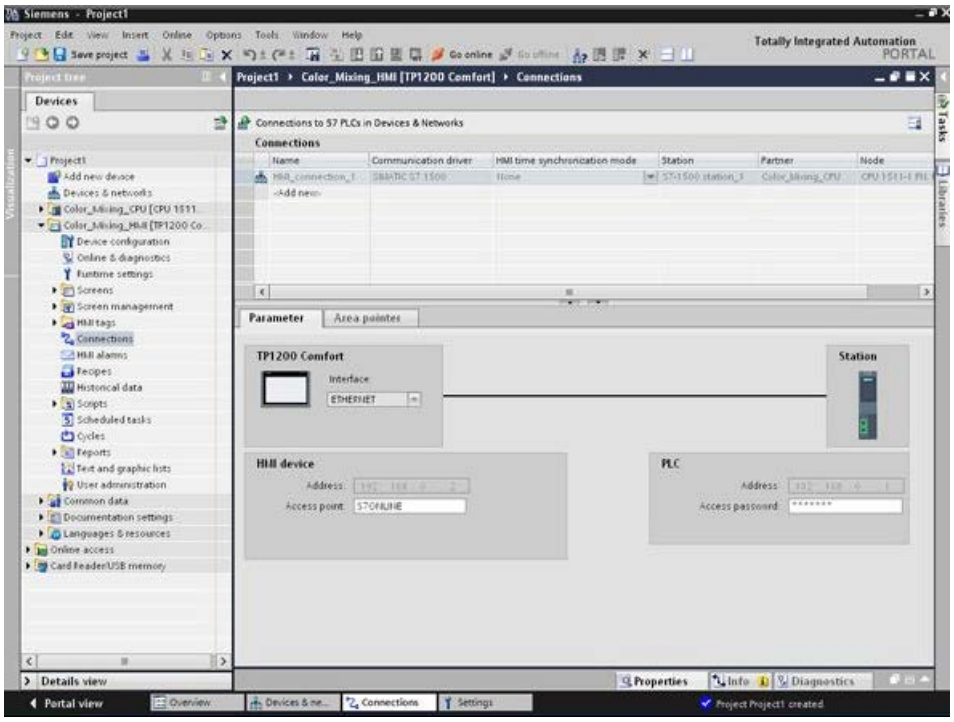
简介

如果 CPU 设置了保护等级“完全保护”，HMI 设备只能访问已存储密码的 CPU。

仅可在 SIEMENS 的 HMI 设备上使用此功能。

步骤

1. 在项目树中打开“连接”(Connections) 编辑器。
2. 选择集成的连接。
3. 在“密码”(Password) 区域中输入 CPU 密码。



结果

HMI 设备现在可以与 CPU 通信并交换数据。