SIEMENS西门子 SINAMICS V60伺服驱动器 6SL31205CC160UA0

产品名称	SIEMENS西门子 SINAMICS V60伺服驱动器 6SL31205CC160UA0
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:代理经销商 V90伺服驱动器:全新原装 假一罚十 德国:正品现货 实体经营
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

定义存取权限访问功能和机床数据访问级别可以控制对功能和数据区的访问操作。访问级别有 1 到 7 个，1 表示最gaoji别，7 表示最低级别。访问级别 1 到 3 通过密码锁定，4 到 7 通过钥匙开关位置锁定。访问级别锁定方法 区域 数据级1 密码：SUNRISE 机床制造商 制造商（M）2 密码：EVENING 维修 个人（I）3 密码：CUSTOMER 用户 用户（U）4 钥匙开关位置 3 编程员、调试员 用户（U）5 钥匙开关位置 2 gaoji操作员 用户（U）6 钥匙开关位置 1 中级操作员 用户（U）7 钥匙开关位置 0 初级操作员 用户（U）Linux 密码 / NCK级别 用户名 UID1 manufact 1022 service 1033 user 1044 operator3 1055 operator2 1066 operator1 1077 operator 108和上表列出的用户一一对应的是同名的用户组，用户组的 GID 和用户的 UID 也一样。一个用户既是其本身同名用户组的成员，同时也是所有其他更低级别用户组的成员。比如：用户 “ operator2 ” 是用户组 “ operator2 ” 的成员，也是用户组 “ operator1 ” 和 “ operator ” 的成员。区分用户组主要用于管控对文件的访问权限。注意不安全密码可导致数据滥用密码设置的不安全，很容易导致数据被滥用。不安全的密码很容易被破解。为方便调试，文档中提供了默认的标准密码。 务必在调试期间修改默认的标准密码。 定期更换密码。 版本低于 V4.8 的数控软件：除了 SINUMERIK Operate 密码外，在调试时还须一并更改 Linux密码。更多信息参见 “ NCU 操作系统 ” 调试手册。 如果没有修改标准密码，SINUMERIK ONE 上会一直显示一条警告。关于安全密码设置的详细信息请参见章节 “ 密码 (页 50) ” 。说明SINUMERIK Operate 与 Linux 密码一同修改从软件版本 4.8 SP3（840D sl/828D）和软件版本 6.13（SINUMERIK ONE）起，SINUMERIK Operate 和 Linux 的访问级别合二为一。如果修改了 SINUMERIK Operate 的密码，Linux 的相关密码也会被一并修改，反之亦然。在该过程中，须注意下列事项： 在执行 NC 清零后，密码不会恢复为标准密码。 在软件升级后，SINUMERIK Operate 密码仍适用于 NC。 密码一经修改，便无法恢复为出厂时的标准密码。 在通过 “ Restore [-full] ” 命令恢复系统时，CF 卡会被格式化，系统恢复为出厂状态。 “ Restore[-full] ” 通过 Emergency Boot System 的菜单项 “ Recover system from USB memory stick(reformat CF card) ” 调用。密码不会包含在 SINUMERIK

存档中。因此，在执行命令 Restore [-full]
后，必须修改标准密码，将它改为自己的密码。产品特殊的安全措施8.1
SINUMERIK工业信息安全配置手册, 01/2023, 6FC5397-5EP40-6RA2 658.1.7.2 Safety Integrated 密码通常
SINUMERIK Operate
中的调试数据是通过不同的访问级别来保护的。和安全相关的驱动参数另外还可以通过 Safety Integrated
密码来保护。该密码保存在驱动数据中，以确保只有掌握密码的授权人员才可以修改这些数据。说明SIN
UMERIK 安全功能上必须使用 SINAMICS 安全密码从 V4.8 SP2 HF1 版本起，您可以通过 SINUMERIK
Operate 画面来设置 Safety Integrated 密码。您同样也可以通过 SINUMERIK ONE Commissioning Tool
的画面来设置 Safety Integrated密码。 请设置安全密码，避免参数被外部配置软件 STARTER 或调试软件
SINAMICS Startdrive 修改。更多信息关于如何修改各个访问级别的密码以及程序、软键、文件各自需要
哪些访问级别或权限的更多信息数控锁功能通过“ 数控锁功能 ”，机床制造商可利用通过 SINUMERIK
Integrate 应用程序 AccessMyMachine (AMM) 创建的加密文件来激活控制系统的锁定日期。该锁定日期就
是机床使用期限的截止日。一旦锁定日期到期，数控锁功能便会阻止系统启动。数控锁功能由此实现了
一种限期使用系统的商业模式，它可以防止系统超期使用。说明仅在 SINUMERIK 828D
上提供注意，数控锁功能只在 SINUMERIK 828D 系统上提供。产品特殊的安全措施8.1
SINUMERIK工业信息安全66 配置手册, 01/2023, 6FC5397-5EP40-6RA2关于数控锁以及如何创建加密
Lockset 文件的详细信息，请参见：删除预装的 SSH 密钥应用场合删除西门子预装的 SSH
密钥，可以降低数据滥用风险。您可以定义和安装自己的 SSH
密钥，确保有足够的权限访问系统。服务命令服务命令‘ sc ’是一个在 SINUMERIK NCU
上执行不同服务任务的工具。语法： sc clear preinstalled-keys可选择的名称： ---访问级别：
service该命令可删除控制系统上由西门子预装的所有 SSH
密钥。服务系统（系统镜像盘）打开后，该命令只删除 CF 卡上的密钥，而不会删除系统镜像盘本身的
SSH 密钥。PLC 的网络服务器PLC 在出厂时没有设置任何密码，PLC 网络服务器也未被激活。说明
当您在 S7 项目中激活 PLC 网络服务器时，必须为 PLC
网络服务器创建对应的用户和密码。请设置一个安全密码。在设置密码时，请参见“ 密码 (页
50) ”一章中的说明。 通信只允许使用 HTTPS
协议，以保证通信的保密性和完整性。软键的访问级别软键的显示和操作不仅可以由 OEM 封锁，也可
以由用户封锁，使操作软件更加符合实际功能范围的需要，也使操作界面更加清晰简单。系统的功能范
围因此会有所缩减，但可以阻止对操作软件功能的访问，减少用户误操作的几率。说明软键访问级别修
改的作用范围在 PCU 上设置软键访问级别仅作用于各个 PCU 软键本身。如果想实施对 NCU
的访问权限控制，无论是制造商还是用户，都必须采取合适的保护机制，并设置相应的权限。BIOS 和
AMT 的访问保护请设置一个高强度 BIOS 密码，以防范对 PCU 50 和 SIMATIC IPC 的 BIOS
的非授权访问，详见“ 密码 (页 50) ”一章。更多信息关于 PCU 50 BIOS 设置的更多信息请查看 PCU
基础软件调试手册设置 AMT (Intel Active Management Technology) 的密码“ Active Management
Technology ”（AMT）功能用于 PCU 的远程管理。在远程管理设备时须采取合适的措施，比如：网络分
段，以确保设备安全运行。出于安全原因，AMT 在 PCU 交付时是关闭的。在 BIOS
安装程序中第一次激活 AMT 时，必须设置一个强保护密码，防止远程管理功能被滥用。使用 Create My
Config（CMC）时的密码保护注意权限设置不当可导致数据滥用访问数据可能会被盗取并滥用，此类数
据比如有：预先配置的、用于访问控制系统的密码。 请采取一些组织管理上的措施，确保只有授权人员
才能访问这些文件。说明链接了外部文件时设置密码保护CMC
中实现的保护机制（即密码保护）不能作用于 CMC 中链接的外部文件。说明防止 CMC
数据包被再次导入注意，您必须通过密码来防止 CMC 数据包被再次导入。
因此，在每次为新项目设置密码时，也须设置一个防止再次导入的密码。专有技术保护在 SINUMERIK
上提供以下保护功能，可以保护您的工艺机密，防止未经授权的访问：SINUMERIK Integrate Lock
MyCycles功能“ SINUMERIK Integrate Lock MyCycles ”（循环保护）可以用于控制系统上循环的加密和保
存。循环加密是通过控制系统外部的程序“ SINUMERIK Integrate Access MyMachine/P2P ”完成的。这种
加密循环在控制系统中的执行不受限制，但为保护厂商的专有技术，加密循环不能被查看。SINUMERIK
808D、828D、840D sl 和 SINUMERIK ONE 上可以安装该软件选件。 说明SINUMERIK 840D sl 中集成的
CP 不支持“ 模块访问保护/保护等级 ”选件。程序块加密自 STEP 7 版本 5.5 SP3、840D sl/ 840D sl
的系统软件版本 V4.5 SP2、SINUMERIK ONE 的V6.13 起，可为功能和功能块在离线视图和在线视图中设
置加密保护。使用该功能可对程序块进行加密，防止对程序块代码的外部访问。在加密时，为

SINUMERIK 系统选择“ SINUMERIK ”，一些情况下还需要选择“ SIMATIC ”。OPC UAOPC UA（Unified Architecture）是一种用于访问控制系统数据（例如通过主系统）的标准工业通信协议。使用软件选件“ SINUMERIK Integrate Access MyMachine /OPC UA ”，可以通过该通信协议读/写 SINUMERIK 840D sl、SINUMERIK 828D 或 SINUMERIK ONE 中的变量。和客户端之间的不安全连接可导致数据滥用和 OPC UA 客户端之间采取非加密连接，可能会导致数据滥用。 因此，每次须加密连接到 OPC UA 客户端。关于如何加密数据连接的说明请参见 SINUMERIK Access MyMachine /OPC UA 配置手册注意用户管理不当或权限分配不当可导致数据滥用用户管理不当或权限分配不当是一个巨大的安全隐患，因为用户此时可以访问原本他没有权限的数据，或执行一些非授权的操作。 请您仔细权衡，作出决定，哪些用户需要哪些权限。作为管理员，您有责任保证正确的用户管理和权限分配。说明选择安全密码请设置安全密码来连接 OPC UA 客户端！关于如何选择安全密码的更多信息，参见章节“ 密码(页 50) ”。TIA Portal 中的用户管理TIA Portal 为项目提供了用户管理功能。该功能可以防止项目被意外或非法更改。用户设置项目保护后，便可以激活用户管理。设置项目保护的该用户因此成为“ 项目管理员 ”。在激活了项目保护后，该项目便只能由授权用户打开并编辑。注意，项目保护一旦设置便无法取消。TIA Portal 提供的用户管理功能适用于控制系统 SINUMERIK 840D sl 和 SINUMERIK ONE。UMC - User Management Component另外，您还可以在一台或多台计算机上安装软件包“ User Management Component UMC ”，它提供了统一的用户管理更多信息关于安全用户管理的更多信息请查看 TIA Portal 的在线帮助。SIMATIC Logon用户管理和可追溯性“ SIMATIC Logon ”选件包用于设置对 STEP 7 中项目和库的访问权限。为某项目设置访问权限后，只有授权用户才可以访问该项目。SIMATIC Logon 可以和 SINUMERIK STEP 7 组合使用。详细信息参见章节“ 通过“ SIMATIC Logon ”实现安全的访问控制(页 97) ”。数据备份在 SINUMERIK 中，不同组件采取不同的存档格式和方法。备份数据的时间点需要备份数据的时间点有： 调试结束后 更改了机床特有设置后 更换硬件组件后 软件升级之前和之后 激活存储器配置机床数据之前请遵守安全数据保存的一般规定中关于存档的说明，详见章节“ 数据保存(页 49) ”。注意将机密数据保存在系统上可导致滥用机密数据如果保存在控制系统上，有潜在的滥用风险。因此，请勿将机密数据导入到控制系统中，比如：通过软件“ SINUMERIK Integrate AccessMyMachine/P2P ”导入。 机密数据必须总是加密保存到本地盘上。机密数据需要保存到某网络文件夹中时，该文件夹也要一并加密。废弃处理注意数据没有安全删除可导致数据滥用产品存储卡或硬盘上的数据如果没有彻底删除或者没有安全删除，可能会导致加工程序、存档等数据被第三方滥用。因此，在废弃产品前，必须事先安全地删除所有使用的存储设备上的数据。 有一些程序可以协助您完成存储设备的安全删除或格式化。当然您也可以委托专业的废弃物处理公司，安全废弃设备。CNC Shopfloor Management Software本章将为您概括介绍一些为防范网络攻击、保护您的 CNC Shopfloor Management Software产品而可以采取的安全措施。关于安全措施的详细说明以及具体步骤请查看对应的 CNCShopfloor Management Software 文档。系统概述CNC Shopfloor Management Software，CNC 车间管理软件，具有面向未来的 IT 架构，由三个层级组成：“ 云端 ”（In Cloud）、“ 产线端 ”（In Line）和“ 机器端 ”（In Machine）。这些层级分别部署在三个平台上：MindSphere、MCenter 和 SINUMERIK/SINUMERIK Edge。整套系统从系统到云端都设计了大量定制功能。云端应用程序（In Cloud）MindSphere 可以提供最先进的信息安全技术，无论是现场的数据采集，还是数据到云端的传送以及数据在云端的保存。它的安全框架融合了 IEC 62443、ISO/IEC 27001 和德国 BSI 标准等行业标准的原则以及官方发布的云平台数据处理建议。MindSphere 和客户端之间经由公共端点的全部通信都采用 TLS 1.2 协议，该协议在工业领域内久经验证。它使用西门子信任中心颁布的 X509 证书，符合欧洲电信标准化协会 ETSI 和CA/B 论坛的要求。该平台通过西门子选择的云基础设施服务商来部署，数据始终保存在服务商云计算数据中心的强大服务器中。所有云计算数据中心都符合最高的数据安全标准，能够防范网络攻击。作为云计算 IaaS（Infrastructure as a Service：基础设施即服务）商业服务商，云基础设施服务商可以提供更高的安全标准，高于通常的个人本地数据保存设备。这些云计算数据中心的运营借鉴了工业行业的zuijia实践经验。为增加一道安全防线，云基础设施服务商还须在现场采取额外的一些保护措施，比如：电子照片/ID 卡验证、持卡人访问控制、生物识别技术、含记录和报警功能的数字式监视器等。