西门子6AU1425-0AA00-0AA0

产品名称	西门子6AU1425-0AA00-0AA0
公司名称	湖南西控自动化设备有限公司
价格	.00/件
规格参数	西门子:全新原装正品 6AU:24小时咨询询价在线 德国:西门子授权代理商
公司地址	中国（湖南）自由贸易试验区长沙片区开元东路1306号开阳智能制造产业园（一期）4#栋301
联系电话	17838383235 17838383235

产品详情

西门子PLC程序加密方法汇总讲解

大家都知道，很多品牌PLC的程序都可以通过软件解密，那么一旦解密后程序就非常透明的显示在了别人的眼中，而将设备卖给别人又将PLC程序整个锁死的话又不切实际，甲方会无法维护；而保密和维权更是中国市场经久不衰的话题，其实德国的工程师从来不会给自己的程序整体加密，而是使用其他方式，既不影响发生故障时的诊断，又可以保护自己的核心机密。给大家介绍一下这些方式，供大家参考。

01使用西门子安全PLC或者博途的KNOWHOW功能

西门子安全PLC作为西门子主打安全功能的一款产品，它的性能毋庸置疑，而且安全PLC的程序块加密后无法破解；可以很好的保护核心。

博途PLC作为西门子的新产品，其版权保护也是它的主要功能之一，KNOWHOW功能是软硬件双重加密，不加密的块可以正常监控，没有密码的话甚至无法下载到其他PLC；因此使用博途的KNOWHOW功能既可以将程序交给甲方方便维护，又可以保护自己的核心程序不被窃取。

02采用语言编写部分重要的工艺程序

西门子除了基础的LAD梯形图编程，FBD功能块编程和STL语句表编程还有很多其他的方式，比如说PCS7的CFC,SFC; 除此之外还有SCL，S7-GRAPH等等。对于这些语言，一般的工控人员很难全部精通，因此仿制难度大大提升，因此非常关键的工艺程序可以由这些语言编写，也可以很好的保护自己的核心。

1、编程方式的采用

a)采用模块化的程序结构，采用符号名，参数化来编写子程序块

b)尽量采用背景数据块和多重背景的数据传递方式

c)多采用间接寻址的编程方式

d)复杂系统的控制程序尤其是一些带有顺序控制或配方控制的程序，可以考虑采用数据编程的方式，即通过数据的变化来改变系统的控制逻辑或控制顺序。

用户应该尽量采用以上几种层次的编程方式，这样编出来的程序中嵌入系统的保护加密程序，才不容易被发现而仿制。

2、主动保护方法

a)利用系统的时钟

b)利用程序卡或者CPU的ID号和序列号

c)利用EEPROM的反写入功能，及一些需要设置的内存保持功能

d)利用系统提供的累时器功能

e)在用户程序的数据块中设置密码

f)软件上设置逻辑陷阱

g)可以反向利用自己在编程时犯的错误

3、被动保护方法

a)在内存容量利用许可的条件下，不要删除被认为是无用的程序

b)在数据块里留下开发者的标识，以便于将来遭到侵权时可以取证

4、应用反窃取技术的注意事项

a)在用户程序中嵌入保护程序要显得自然一些，不能很突兀的加出一段程序来，代码要尽量精简，变量符号名应与被嵌入程序段的变量保持一致

b)往往一种保护加密手段是不够的，应该多种方法并用，并且这些保护程序一旦激活后对系统造成的后果也应该尽量不同，造成所谓的“ 地雷效应 ”，从而增加程序被窃取的难度，时间与成本，短时间内让抄袭者束手无策，

c)保护好程序的原代码，如果需要交付程序的，在不影响用户对设备维护的前提下，应对交付的程序做适当的技术处理，如删除部分符号名，采用上载的程序或数据块

d)做好严格的测试，以避免保护程序的不完善引起的误动作而带来的不必要的麻烦，同时也能降低售后服务的的费用。

03使用通讯功能

在实际应用中，往往会遇到一些系统间需要数据交换的问题(多个PLC之间，PLC与第三方仪表之间)，无论是西门子产品之间还是西门子产品与第三方产品之间，建议使用通讯的方案来代替模拟量或开关量之间的信号互连的方案。

对于前者，仿制者只能看见一条硬件的通讯线，至于有多少数据是如何通过通讯交换的，仿制者必须要花精力研究具体的用户程序才能搞清楚;而对于后者，开发者是省心省力了，仿制者也是一目了然，尽收眼底。

对于一些变频器或者伺服电机等的程序设计，一般有多种方式，可以线路直接控制还可以通讯控制，那么使用通讯的方式的话会使得程序增加了仿制的难度，比如说PLC对于伺服驱动器的控制有多种，简单一些的可以是脉冲直接控制或者模拟量控制，这种方式就容易仿制，如果换成通讯控制，则会使得程序复杂很多，加上仿制者如果对报文不熟悉，很难去仿制。

有时候控制系统会由多个子控制系统构成，由此形成多CPU加人机界面的网络，西门子S7-200产品常见的是PPI网络，S7-300400产品常见的是MPI网络，通常是人机界面与CPU之间的数据交换，而我们也可在CPU的用户程序中添加一些无须组态的S7基本通讯功能(S7-200可用NETRNETW指令，S7-300400可以用X_PUTX_GET指令)，定时或不定时地在CPU之间进行少量数据交换，通过这些数据实现子系统控制逻辑的互锁。对于这样的系统，仿制者要分析某一子系统的程序也不是件十分容易事情。

04采用面板类型的人机界面

尽量在自动化系统中使用面板类型的人机界面来代替单一的按钮指示灯，很多人机界面没有源程序的话只有备份和恢复功能，完全可以实现维护功能还保密了HMI这一层的程序，而对于一个PLC系统而言，即使拥有了源程序但是缺失了HMI部分的标记也是很难仿制的。

而且开发者可以在面板的画面上加上明显的厂家标识和联系方式等信息，仿制者就不能原样照抄。

如果就使得如果仿制者想要复制程序的话，就必须重新编写操作面板的程序甚至于PLC的程序，而开发者则可利用面板和PLC数据接口的一些特殊功能区(如西门子面板的区域指针，或VB脚本)来控制PLC的程序执行。这样的PLC程序在没有HMI源程序的情况下只能靠猜测和在线监视来获取PLC内部变量的变化逻

辑，费时费力，极大的增加了仿制抄袭的难度。

05采用非标准的人机界面

德国工程师都愿意使用这种方式。在中国，大多数工程师都愿意使用WINCC，INTOUCH或者组态王等等，但其实除了这些软件，还有一种更加高大上的编写方式，那就是利用VB自己写程序，而对于软件与PLC的接口，大家可以选择LIBNODAVE或者其他库等，这种方式写出来的人机界面有着很多好处，首先没有版权问题，因为VB软件是免费的，而且对于WINDOW系统的升级来说只需要简单的添加几个文件即可实现，不像WINCC那样，如果window升级了，需要大量修改文件。

一般人都无法修改，更别提仿制了；没有很好的计算机编程功底的话就不敢轻易修改，而仅仅有计算机功底又没有PLC或者工艺基础的话也是无法更改的。