化工自动化及仪表，2006，33(2):39～41
Control and Instruments in Chemical Industry

C/S模式下应用C及VBScript语言实现WinCC组态加密

陈东宁，姜万录

（燕山大学 机械工程学院，河北 秦皇岛 066004）

摘要： 综合运用ANSI-C和VBScript语言编制加密程序，实现了执行动作的授权化、组态环境和运行环境的分离以及运行环境的安全退出等功能。设置WinCC组态参数，实现了工程脚本的加密、Windows热键的屏蔽以及运行窗口关闭等常规按钮的消隐。

关键词： WinCC；加密；C/S模式；C；VBScript

中图分类号： TP31　**文献标识码：** B　**文章编号：** 1000-3932(2006)02-0039-03

1 引 言

WinCC是西门子公司推出的监控组态软件，它集成了SCADA、组态、Script语言、ActiveX和OPC等先进技术，为用户提供了Windows操作系统环境下使用各种通用软件的功能[1]。作为SIMATIC全集成自动化系统的重要组成部分，WinCC确保了与SIMATIC S5、S7和505系列PLC以及TDC连接的方便和通讯的高效，被越来越广泛地应用于化工、冶金、水电等领域[2~4]。

WinCC组态环境和运行环境没有完全分离，软件使用者可以轻易进入组态环境，查看源程序，修改组态界面。而对于工程项目，软件组态环境的加密是十分重要的。一方面，加密可以保护工程软件编写人员的知识产权，对其劳动成果加以尊重；另一方面，可以防止未经授权的人随意改动程序而造成的经济损失和安全事故。

通过某工厂的实际项目设计，本文深入系统研究了C/S(Client/Server)模式下WinCC软件组态环境的加密问题。

2 C/S模式的使用

本项目使用的是WinCC V6 SP2 ASIA，操作系统为Windows XP。采用C/S模式，配置一台服务器，两台客户机，组态多用户项目。服务器通过TCP/IP协议完成与下位机TDC的实时通讯，接收下位机传送的外部过程数据。服务器进行复杂的运算，并将结果发送给下位机。服务器中WinCC集成了OEM数据库实例SQL Server 2000，可以进行内部变量及外部变量的实时快速归档，以及报警事件的归档。客户机上没有组态项目，只需登录服务器，运行服务器上的项目。因而，客户机不需要购买组态授权，只需一定点数的运行授权即可，这种模式可以降低软件造价。

在C/S模式下，通过不同的客户机可以观看不同的监控画面，完成监控、报表、历史数据查询等多种功能。然而，在联网状态下任何一台客户机也可轻易地访问服务器的组态环境，可以修改组态界面，更改脚本代码。所以在C/S模式下，保护软件安全更为困难和必要。

3 ANSI-C和VBScript脚本的加密

虽然WinCC提供了标准的智能对象、窗口对象及ActiveX控件等组态工具。但是对于复杂的运算、后台任务等需要借助于脚本来完成。WinCC提供了两种脚本：ANSI-C和VBScript。在画面中组态的对象可以直接输入ANSI-C或者VBScript脚本代码。对于不重要的代码，采取这种方式比较省事。

对于具有重要功能的代码，应该使用全局脚本编辑器。全局脚本编辑器位于WinCC资源浏览器下，包括C-Editor和VBS-Editor。需要多次引用或者需要加密的脚本，可以在全局脚本编辑器中编制项目函数(C)或者项目模块(VBS)。在画面中组态对象时，在其属性或者事件中就可以引用这些项目函数或者项目模块。全局脚本编辑器为函数和模块提供了加密功能。打开C-Editor或者VBS-Editor，点击菜单按钮“信息/触发”图标，在弹出的对话框界面为该脚本输入口令。同样，对于动作，也可以输入口令。这样，即使用户进入了组态环境，想更改脚本，也需要输入正确的口令才能看到脚本源代码。

收稿日期：2005-11-02

基金项目：国家自然科学基金项目资助(60374042)

4 应用C脚本对动作进行加密

在生产实际中,一些特殊的按钮,被不熟悉生产工艺的人随意操作,可能会引发安全事故。所以必须为这些按钮分配操作权限。只有被授权的用户,在输入用户名和密码之后,才能执行操作。分配操作权限的操作必须通过用户管理器来完成。

在WinCC运行画面,WinCC提供了热键来自动弹出用户登录对话框。热键需要设置和记忆,加重了编程者和使用者的负担。所以在需要登录用户的地方,设置了按钮,应用ANSI-C语言,编写了弹出输入用户密码的对话框的函数UserPW.fct,代码如下:

```
#include "apdefap.h"
void OnClick (char * lpszPictureName, char * lpszObject-
Name,char * lpszPropertyName)
{
#pragma code("UseAdmin.dll")
#include "pwrt_api.h"
#pragma code()
PWRTLogin('1');
}
```

5 运行系统自动登录

在Windows开始菜单,点击SIMATIC\WinCC\Windows Control Center 6.0,则打开了WinCC的组态环境。这在工程开发阶段是十分方便的。但是项目交付使用之后,再由用户打开组态界面,是没有必要的,也是不安全的。所以要实现运行环境的自动登录。

5.1 开机自动登录

实现自动登录功能的过程如下:在Windows开始菜单,点击SIMATIC\WinCC\AutoStart,则出现AutoStart组态对话框。在WinCC安装路径,找到扩展名为MCP的工程项目并添加。在"启动时激活项目"提示行前面的方框里面不划勾,则开机自动进入WinCC的运行画面。在"激活时允许'取消'"前的方框中不划勾,这样防止进入运行阶段的等待过程中用户取消激活,又将进入到组态环境。点击"添加到AutoStart",并点击"确定"按钮则组态成功,该项目在开机进入windows之后WinCC会自动运行,直接进入运行画面,不出现组态环境。组态自动登录AutoStart的界面如图1所示。

在C/S模式下,对于客户机,需要与服务器保持网络连接,找到网络上服务器的项目路径,添加服务器的MCP工程项目。这样在服务器项目正常运行下,客户机开机进入Windows后,就会自动进入服务器中WinCC项目的运行画面。

5.2 快捷方式自动登录

如果不希望开机自动运行进入WinCC,而在其它时间进入工程项目的运行界面,则可以在桌面上右键建立快捷方式。在WinCC安装目录下的bin文件夹中找到AutoStartRT.exe可执行文件,并在AutoStartRT.exe文件名后面输入服务器项目的MCP文件路径,加上参数\Activ:yes\LANG=CHS,建立快捷方式。双击快捷方式的图标即可进入WinCC的运行界面。

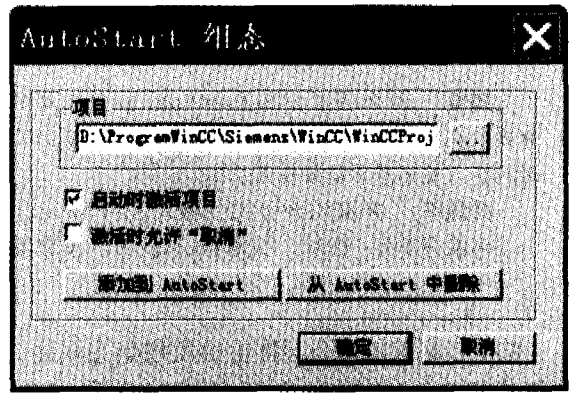

图1 组态自动登录AutoStart界面

5.3 Windows快捷键的屏蔽

完成了组态环境和运行环境的分离,用户即可直接进入运行环境。但是如果用户通过运行画面右上角的最小化或者关闭按钮,那么同样可以离开运行环境,进入组态环境,所以要将这些按钮去掉。在WinCC资源管理器下,在"计算机"图标上单击右键,设置计算机属性。在"图形运行系统—关闭"子目录下,将"关闭"、"最小化"等前面的方框勾上,这样,运行界面中就不会出现关闭画面等按钮了。

Windows自带了一些用于退出程序的热键,或者弹出Windows界面的热键,对于Windows操作系统比较熟悉的人员可以利用这些热键来退出WinCC运行环境,所以需要将这些热键禁止掉。还是在设置计算机属性的窗口下,点击"参数",将禁止键"Ctrl+Alt+Del"等前面的方框勾上,就可以禁止这些键的作用。一般的工程人员可能会忽视这些Windows热键的屏蔽。

6 C/S模式下运行系统的退出

当应用软件交付之后,软件编制者由于某种原因,需要修改源程序,那么需要退出运行系统。而在C/S模式下,所有的服务器和客户机运行窗口右上角都去掉了最小化或关闭的按钮。Windows热键也已经被屏蔽了。这时再退出运行界面,就需要编程人员给自己留一个退路。本文结合C及VBScript语言的优势,编写脚本开发了安全退出WinCC运行环

境的程序。其编程思路及脚本如下：

该项目的主菜单画面为Picture1。在Picture1中调用了WinCC的库对象Group1，是按钮Button1和状态显示StatusDisplay1的组合，StatusDisplay1引用了一个小人跑出房间的图片。按钮Button1属性中“文本”一项输入“退出”。

在Picture1添加一个智能对象画面窗口PicWind，在PicWind属性“显示”中与WinCC内部二进制变量Bit1相连。画面名称静态属性中输入PicExit.pdl。

在按钮Button1的鼠标动作事件中，将Bit1的值设置为1，编写的VBS脚本如下所示：

```
Sub OnClick(ByVal Item)
HMIRuntime.Tags("bit1").Write 1
End Sub
```

这样在点击Group1后，退出WinCC的PicExit.pdl画面就可以出现。

在PicExit.pdl画面中，添加了三个按钮Button2、Button3和Button4。Button2用来输入密码，字体属性中输入“输入密码”，在鼠标动作的事件中引用C-Editor中编写的项目函数UserPW.fct，单击该按钮就可弹出输入用户名和密码的对话框。

Button3属性中“字体”一项在静态属性输入“确认退出”，属性中“授权”一项的静态属性选择“动作编辑”。“动作编辑”授权的用户名和密码事先通过“用户管理器”进行了设置。Button3事件中“鼠标动作”中编写的C脚本如下：

```
#include "apdefap.h"
void OnClick ( char * lpszPictureName, char * lpszObjectName,char * lpszPropertyName)
{
  DeactivateRTProject();
}
```

在编程者已经正确登录后，则单击按钮Button3可退出WinCC运行环境。

Button4属性中“字体”一项在静态属性中输入“取消退出”，右键属性中为鼠标事件添加脚本，Bit1置零。在用户非法或者不想退出运行环境的情况下，按下该按钮，则隐藏退出运行环境的画面窗口PicExit.pdl，退出过程被取消，恢复了主菜单原来的状态。应用VBS开发的脚本如下：

```
Sub OnClick(ByVal Item)
HMIRuntime.Tags("bit1").Write 0
End Sub
```

点击小人图标，PicExit.pdl中的部分画面在主菜单界面Picture1中嵌套显示，如图2所示。

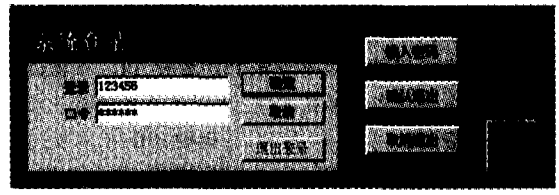

图2　退出WinCC运行环境界面

7　结　论

针对WinCC软件开发的项目，完成了整体调试和加密工作，并应用于实际生产中，极大地提高了生产运行的安全性，得到了用户的理解和支持。本文是在进行实际项目过程中不断摸索和总结的加密技巧，其中有些技巧不光有益于WinCC软件的使用者，对其他工程软件使用者也会有所裨益。相信随着工程组态软件的日趋完善，加密技术也会更加安全和有效。

参考文献：

[1] 西门子(中国)有限公司自动化与驱动集团. 深入浅出西门子WinCC V6[M]. 北京：北京航空航天大学出版社，2004.

[2] 高德欣，张文武，杨　清. 基于C/S模型的OPC客户端实现WinCC数据转储[J]. 化工自动化及仪表，2005，32(5)：33-36.

[3] 王书锋，王　云，邹益仁. 青岛发电厂化学补给水处理计算机监控系统[J]. 化工自动化及仪表，2001，28(2)：36-39.

[4] 万健如，刘春江，刘洪池，等. 涂料化工生产过程自动监控[J]. 化工自动化及仪表，2002，29(4)：58-60.

Realizing WinCC Configuration Encryption Using C and VBScript in C/S Model

CHEN Dong-ning，JIANG Wan-lu

(*College of Mechanical Engineering，Yanshan University，Qinhuangdao* 066004，*China*)

Abstract：According to the application of WinCC，the principle and method of project software encryption in C/S model are presented. The encryption procedure is compiled using VBScript and ANSI-C language，which accomplishes the authorization of operation，separation of configuration and operation environment，and safe withdrawal function. The configuration parameters are established to realize script encryption，shielding of Windows hotkeys and hide of conventional buttons such as close windows. The safety of software is enhanced and the running of production is guaranteed.

Key words：WinCC；encryption；C/S model；ANSI-C；VBScript