POSITIVE TECHNOLOGIES

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107241 / МОСКВА / ЩЕЛКОВСКОЕ ЩОССЕ / Д.23А
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

SIEMENS SIMATIC WINCC 7.X

SCADA SECURITY HARDENING GUIDE
DRAFT VERSION

ОГЛАВЛЕНИЕ

1. НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ

1.1 Использование совместимой версии Windows

Не рекомендуется производить установку WinCC 7 и дополнительные компоненты на неподдерживаемые производителем операционные системы.

Рекомендации:
Проверить соответствие операционной системы согласно таблице:

http://support.automation.siemens.com/WW/llisapi.dll/csfetch/21927773/WinCC_V70_compatibility_list_e.pdf

Software \ WinCC Version		SIMATIC WinCC V7.0							
		V7.0		V7.0 SP1		V7.0 SP2		V7.0 SP3	
		Client / Singlestation	Server	Client / Singlestation	Server	Client / Singlestation	Server	Client / Singlestation	Server
Microsoft Windows (32-Bit)	Windows 7 *11)					x			
	Windows 7 SP1 *11)							x	
	VISTA *5)	x							
	VISTA SP1 *5)			x					
	XP Professional SP2	x	x *16)	x	x *16)				
	XP Professional SP3			x	x *16)	x	x *16)	x	x *16)
	Server 2003 SP2 *4)	x *14, 15)	x	x *14, 15)	x	x *14, 15)	x	x *14, 15)	x
	Server 2003 R2 SP2 *4)	x *14, 15)	x	x *14, 15)	x	x *14, 15)	x	x *14, 15)	x
	Server 2008 SP2 *4, 17, 19)					x *15)	x	x *15)	x
Microsoft Windows (64-Bit)	Windows 7 SP1 *11)							x	
	Server 2008 R2 SP1 *4, 19)							x *2)	x
Virtualization	VMware ESXi 4.0					x	x	x	x
	Windows Server 2008 Hyper-V					x			
	Windows Server 2008 R2 Hyper-V							x *2)	x

2) Only released for WinCC Singlestation
4) Standard and Enterprise Edition
5) Ultimate / Business / Enterprise
11) Professional, Enterprise and Ultimate
14) Clients without own project are not allowed for operating system Windows Server 2003 (R2).
15) Windows Server is only released as a WinCC Client operating system if the WinCC Server operating system is not Windows XP.
16) Only for WinCC Server projects and max. 3 clients. See "WinCC Information System > Configurations > WinCC ServiceMode" and "WinCC Information System > Release Notes > Notes on Process Control Options > Server Project on Windows XP with Clients without their own project".
17) Please consider the following link for a optionally downgrade of Windows Server 2008 R2:
http://www.microsoft.com/windowsserver2008/en/us/downgraderights.
Aspx
19) Microsoft Windows Server 2008 without Hyper-V is not allowed.

Дополнительно возможно воспользоваться порталом поддержи и проверить совместимость различных продуктов Siemens:

https://support.automation.siemens.com/kompatool/pages/main/index.jsf

1.2 Совместимость WinCC 7 с другими компонентами и программным обеспечением

Установка лишних или не совместимых продуктов, компонентов ОС, программного обеспечения Siemens для работы WinCC 7 не рекомендуется производителем.

Проверить полный список совместимости компонентов и продуктов можно:
http://support.automation.siemens.com/WW/llisapi.dll/csfetch/21927773/WinCC_V70_compatibility_list_e.pdf

Примечание:
Параллельная установка WinCC 7 Flexible 2008 возможна со следующими продуктами серии SIMATIC: WinCC Basic V11, WinCC Comfort V11, WinCC Advanced V11 и WinCC v11 Professional, STEP 7 V5.4 или V5.5, STEP 7 Micro/WIN, STEP 7 10.5, STEP 7 11, WinCC Flexible 2008.

Рекомендации:
Проверить состояние установленных компонентов можно следующим образом: Start -> Control Panel -> Add or Remove Programs -> Add/Remove Windows Components

1.3 Некорректная настройка языковых параметров Windows

Работа WINCC рекомендована только для перечисленных ниже языков операционной системы:

- Немецкий
- Английский
- Французский
- Итальянский
- Испанский
- Многоязычная операционная система*

* Для систем MUI языком операционной системы является английский

Примечание:
Установка WINCC на операционные системы с неподдерживаемыми языками возможна, но тогда могут возникнуть проблемы с некорректным отображением экранных шрифтов, либо со стабильностью работы самого продукта.

Рекомендации:
Проверить используемый язык системы Start -> Control Panel -> Regional and Language Options

1.4 Установлены последние обновления Windows

Для поддержания актуального уровня безопасности операционной системы Windows, должны быть установлены все актуальные обновления (hotfix), помеченные Microsoft как ”критические” и ”важные” (“critical” и ”important”) и проверенные корпоративной службой ИТ.

1.5 Не разрешить установку драйверов и файлов без подписей после установки WinCC Advanced TIA Portal

Для корректной установки и настройки программного обеспечения WinCC Advanced TIA Portal на операционной системе Windows, необходимо отключить стандартную проверку на установку драйверов использующих цифровую подпись. После установки WinCC Advanced TIA Portal нужно обязательно включить проверку цифровой подписи.

Рекомендации:
Start -> Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies ->Security Options
Проверьте настройки политик безопасности:
– Windows Vista
– Windows XP/Windows Server 2003 (Devices: Unsigned driver installation behavior).
Для политик выберите параметр Accept without или Warn, but permit installation.

1.6 Использовать функции предотвращения выполнения данных

Необходимо использовать функции предотвращения выполнения данных Data Execution Prevention (DEP) для всех приложений в Windows. Функция безопасности, встроенная в Windows, которая не позволяет приложению исполнять код из области памяти, помеченной как «только для данных». Она позволит предотвратить некоторые атаки, которые, например, сохраняют код в такой области с помощью переполнения буфера.

Рекомендации:
Данную функцию, возможно, отключать на время проведения установки, наладочных работ или на этапе создания проекта (выборочно сделать ограничения). При использовании исполнительной среды WinCC на постоянной основе, функция предотвращения выполнения данных должна быть включена для всех программ.
Start -> Settings -> Control Panel -> System -> Advanced -> Performance -> Settings -> Data Execution Prevention -> Turn on DEP for all programs and services expect those I select.

1.7 Ограниченное членство в системных группах

Необходимо обеспечить контроль ограничений на членство в системных группах Administrator, Server Operators, Power Users.

Start -> Settings -> Control Panel -> Administrative Tool -> Computer Management -> Local Users and Group

1.8 Распределение прав доступа для WinCC

После установки WinCC система автоматически создает следующие локальные группы в окне управления группами и пользователями Windows:

- SIMATIC HMI. Участники этой группы могут создавать локальные проекты и удаленно обрабатывать и запускать их, а также получать к ним доступ. По умолчанию в эту группу входят пользователь, выполняющий установку WinCC, и локальный администратор. Других участников администратор может добавить вручную.
- SIMATIC HMI CS. Участники этой группы могут выполнять только конфигурацию, но не могут вносить изменения в компоненты среды исполнения напрямую. По умолчанию эта группа пустая и зарезервирована для последующего использования.
- SIMATIC HMI Viewer. Участники этой группы обладают доступом только для чтения данных конфигурации и среды исполнения. Данная группа, главным образом, используется для учетных записей служб Веб-публикаций, например IIS (Информационные службы Интернета), чтобы обеспечить работу WinCC Webnavigator.

Добавьте в группу SIMATIC HMI только тех локальных пользователей, для которых разрешен доступ к WinCC.

Примечания по установке:
http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC/V70/InstallNotes_ru.pdf

Примечание:

Разработчики и пользователи компонентов среды исполнения должны быть зарегистрированы не только в группе SIMATIC HMI, но и в группе Windows. Участники группы SIMATIC HMI могут получать доступ только к проектам, но не к операционной системе. Чтобы создать проект, разработчик должен быть главным пользователем и пользователем группы SIMATIC HMI.
В распределенных системах создаваемые пользователи WinCC должны входить в одни и те же группы и для пользователей на всех компьютерах необходимо назначить одинаковый пароль.

Рекомендации:
Для добавления в группу SIMATIC HMI пользователей, сначала необходимо создать локальных пользователей. (Пользователей домена можно добавить в группу SIMATIC HMI напрямую.)

Start -> Settings -> Control Panel -> Administrative Tools -> Computer Management-> Local Users and Groups -> Users с помощью контекстного меню откройте диалоговое окно New User и создайте учетную запись пользователя с таким же именем для каждого пользователя, которому требуется доступ к WinCC.
Далее перейдите Local Users and Groups -> Groups -> SIMATIC HMI.
С помощью всплывающего меню откройте диалоговое окно Add Member и добавьте этих пользователей, как участников группы SIMATIC HMI.

При использовании домена можно создать дополнительную глобальную группу пользователей домена и добавить ее в качестве участника группы SIMATIC HMI. Для этого:

- Администратор домена должен создать глобальную группу пользователей домена.
- В пределах домена администратор добавляет в домен пользователей, для которых разрешен доступ к WinCC.

Start -> Settings -> Control Panel -> Administrative Tools -> Computer Management-> Local Users and Groups -> Users с помощью всплывающего меню откройте диалоговое окно New User. Создайте учетную запись пользователя с таким же именем для глобальной группы пользователей домена.
Далее перейдите Local Users and Groups -> Groups -> SIMATIC HMI.
С помощью всплывающего меню откройте диалоговое окно Add Member и добавьте глобальную группу пользователей домена как участников группы SIMATIC HMI.

1.9 Предотвращение доступа к уровню операционной системы в среде исполнения

Если в активном проекте WinCC открыто диалоговое окно выбора “Windows” (импорт данных или выбор файлов), с помощью этой функции можно получить доступ к операционной системе Windows. Во избежание несанкционированного доступа к операционной системе защитите соответствующую функцию, выполнив проверку Permission Check (Проверка разрешений) с помощью User Administrator (Администратор пользователей).

Рекомендации:
SIMATIC WinCC Explorer ->*Project Name*-> User Administrator -> Open

Примечания по установке:
http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC/V70/InstallNotes_ru.pdf

1.10 Предотвращение доступа к панели инструментов Windows

С помощью свойств компьютера запретите отображение панели инструментов Windows в среде исполнения. Откройте диалоговое окно SIMATIC WinCC Explorer -> Computer -> Computer properties (Свойства компьютера) и отключите все «горячие» клавиши на вкладке Parameter (Параметр) в разделе Disable Keys (Отключить клавиши). Кроме того, в ОС Windows отключите параметр Keep the taskbar on top of other windows (Отображать панель задач поверх остальных окон).
Примечания по установке:
http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC/V70/InstallNotes_ru.pdf

1.11 Отключение клавиш

При отключении комбинации клавиш, следующие комбинации также отключаются в среде исполнения:

<Клавиша Windows+U> Диспетчер специальных возможностей
Пять раз нажмите <Shift> Функция блокировки
Восемь раз нажмите <правую клавишу Shift> Задержка действия
<левая клавиша Alt+левая клавиша Shift+Num> Управление мышью с помощью клавиатуры
<левая клавиша Alt+левая клавиша Shift+Print> Высокая контрастность

Рекомендации:
Функции можно настроить с помощью Control Panel ОС Windows. При включении функций в Control Panel ОС Windows перед запуском среды исполнения WinCC они не блокируются в среде исполнения.

Подробней о настройках и проверки:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=332356&objAction=csOpen&nodeid0=10805593&lang=en&siteid=cseus&aktprim=0&extranet=standard&viewreg=WW

1.12 Отключение удалённого доступа к компьютеру

Если не требуется использование удалённого доступа к компьютеру, на котором используется исполнительная среда WinCC Flexible, требуется отключить данную функцию в Windows.
Start -> Settings -> Control Panel -> System -> Remote

2. НАСТРОЙКА СЕТЕВЫХ ПАРАМЕТРОВ СИСТЕМЫ

2.1 Запрет доступности к сетям общего пользования

Для максимальной безопасности следует разделить сети для управления, передачи данных и основного назначения. Таким образом, можно избежать компрометации системы при попадании злоумышленника в одну из сетей.

Рекомендации:
Проверить доступность внешних сетей с использованием приложения **netstat** с параметрами **–rn**
Start -> Programs -> Accessories -> Command Prompt -> netstat –rn

2.2 Клиенты Novell Netware не установлены

WinCC не следует устанавливать на систему вместе с программным обеспечением клиента Novell. Установка WinCC может привести к тому, что регистрация в системе Novell или блокировка клавиатуры в среде исполнения станут невозможными.

Рекомендации:
Рекомендуется не использовать программное обеспечение клиента Netware или использовать клиент Microsoft для Netware.

3. НАСТРОЙКА СУБД

3.1 Установлены последние обновления безопасности Microsoft SQL 2005

Рекомендуется устанавливать все доступные на текущий момент исправления и обновления SQL Server.

Убедитесь в том, что установлены все исправления и пакеты обновлений для SQL Server, доступные на текущий момент. В средах с несколькими экземплярами SQL Server исправления должны быть применены к каждому экземпляру.

Установите последние обновления и исправления с сайта производителя.

3.2 Используется сложный пароль системного администратора

В качестве пароля системного администратора сервера SQL можно использовать только символы ASCII. Длина пароля должна составлять не менее 14 символов.

3.3 Используется сложный пароль учетной записи для доступа к СУБД

В качестве пароля для доступа к SQL можно использовать только символы ASCII. Длина пароля должна составлять не менее 14 символов.

3.4 Изменены пароли учетных записей WinCCAdmin и WinCCConnect

В качестве пароля для доступа к SQL (например, учетной записи администратора), можно использовать только символы ASCII. Длина пароля должна составлять не менее 14 символов.

Проверка учетных записей WinCCAdmin и WinCCConnect на использование публичных парольных данных

```
login='WinCCAdmin' password='2WSXcde.'
login='WinCCConnect' password='2WSXcder'
```

3.5 Ограничить пользователям SIMATIC HMI права на доступ к SQL-серверу

Участники группы пользователей ОС Windows “SIMATIC HMI” не должны быть одновременно участниками группы ОС Windows SQLServer2005MSSQLUser$<COMPUTERNAME>$WINCC. Участники этой группы имеют права администратора к SQL-серверу. Для ограничения прав доступа к WinCC в

Microsoft SQL Server 2005, необходимо удалить всех пользователей ОС Windows из группы SQLServer2005MSSQLUser$<COMPUTERNAME>$WINCC.

4. ДОПОЛНИТЕЛЬНЫЕ СРЕДСТВА ЗАЩИТЫ

4.1 Установлено совместимое антивирусное ПО

На операционную систему с установленным программным обеспечением WinCC, рекомендуется устанавливать только совместимое антивирусное программное обеспечение.

Рекомендации:
Проверить соответствие антивирусного программного обеспечения согласно списку:

http://support.automation.siemens.com/WW/llisapi.dll/csfetch/21927773/WinCC_V70_compatibility_list_e.pdf

4.2 Используемое антивирусное ПО обновлено и активно

Необходимо чтобы антивирусное программное обеспечение было активно и использовало актуальную базу обновлений

Рекомендации:
Проверить соответствие антивирусного программного обеспечения согласно списку:

http://support.automation.siemens.com/WW/llisapi.dll/csfetch/21927773/WinCC_V70_compatibility_list_e.pdf

5. SIMATIC SIEMENS WINCC (СИСТЕМНЫЕ ПАРАМЕТРЫ)

5.1 Проверка актуальности последних обновлений

До официального выхода сборников обновлений (SP, Update), Siemens часто выпускает различные официальные обновления для отдельных компонентов WinCC 7. Рекомендуется устанавливать все доступные на текущий момент исправления и обновления WinCC 7.

Убедитесь в том, что установлены все исправления и пакеты обновлений для WinCC 7, доступные на текущий момент.
Установите последние обновления и исправления с официального сайта Siemens.

Рекомендации:
Проветрить последние обновления можно тут:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&siteid=cseus&aktprim=0&extranet=standard&viewreg=WW&objid=10805583&treeLang=en

5.2 Приложение WinCC DiagAgent (CCDiagAgent) не используется в промышленных системах

Приложение WinCC DiagAgent (CCDiagAgent) используется для управления и диагностики Simatic WinCC, операционной системы и СУБД. Стандартно приложение не требует авторизации, что может быть использовано для изменения настроек системы и удаленного выполнения

произвольных программ. Контролируйте, что данное приложение удалено или не запущенно на промышленных системах

Рекомендации:
Контроль отсутствия в процессах операционной системы запущенного приложения **CCDiagAgent.exe**

5.3 WinCC Runtime запускается в качестве системной службы

Необходимо удостовериться, что приложение WinCC Runtime запускается в качестве системной службы.

Рекомендации:
Произвести контроль установок служб в SIMATIC WinCC Explorer -> *Project Name* -> Project properties -> Operation mode -> Service

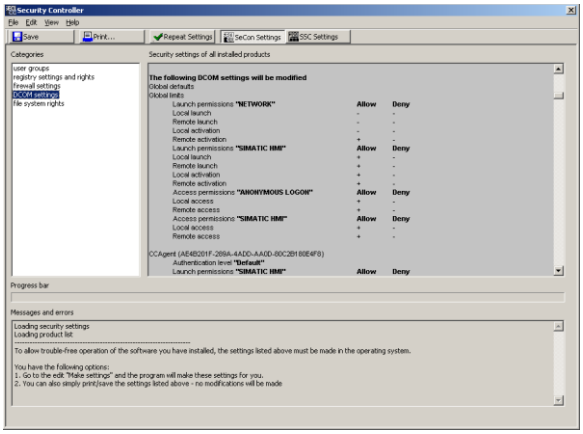
5.4 WinCC Runtime запускается в качестве системной службы

Необходимо удостовериться, что приложение WinCC Runtime запускается в качестве системной службы.

Рекомендации:
Произвести контроль установок служб в SIMATIC WinCC Explorer -> *Project Name* -> Project properties -> Operation mode -> Service

5.5 Дополнительное приложение Security Controller

Дополнительная программа для быстрой перенастройки системных параметров, разрешающая полный доступ для большинства программных продуктов Siemens установленных на компьютере. Также она позволяет сохранить настройки, которые могут быть занесены, в отдельном файле.



Окно Security Controller

Примечание:
Программа, отображает какие изменения, она может занести в систему Windows: изменение параметров в реестре, разрешить входящие ICMP Echo (пинг), разрешить использование файлов и принтеров, изменения параметров DCOM (разрешить ограничения), изменения разрешений в файловой системе.

Рекомендации:
Данные настройки нужны для обеспечения полной работоспособности продуктов фирмы Siemens, но лишь условно называться настройками безопасности. Данной программой можно воспользоваться, если вам нужно сбросить все настройки безопасности, и перенастроить систему заново, но никак не использовать ее после установки WinCC 7.
Данный продукт должен использоваться только компетентным персоналом, либо должен иметь ограничения на использование.

Файлы конфигурации проверок:
C:\WINDOWS\security\SecurityController\
ReturnedFeatures_conv.xml (основной файл отображения)
SeCon.log (файл отчета)


SecurityController.rar

Все файлы:
Файлы программы:
C:\Program Files\Common Files\Siemens\SeCon

5.6 Запрещен параметр отмены загрузки WinCC Runtime

При автозапуске проекта WinCC требуется удостовериться, что параметр Allow "Cancel" during activation приложения AutoStart Configuration деактивирован.

Рекомендации:
Произвести контроль установки флагов активации путем запуска приложения AutoStart Configuration "Program Files\Siemens\WinCC\bin\AutoStartRT.exe"

Произвести контроль значения EnableBreak реестра Windows.

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Siemens\WinCC\AutoStartWinCC]
"ProjectName"="C:\\Users\\Public\\Documents\\Siemens\\WinCCProjects\\123\\123.MCP"
"Activate"=dword:00000000 - Значение Activate project at startup
"EnableBreak"=dword:00000001.
"AllUsers"=dword:00000000 – доступно всем пользователям
"NCGM"=dword:00000000
"RedProject"=dword:00000000
"RedProjectName"=""
"StartInServiceMode"=dword:00000000

6. SIMATIC SIEMENS WINCC (НАСТРОЙКИ SIMATIC LOGON)

6.1 Установлен тайм-аут входа в систему

При использовании приложения SIMATIC LOGON требуется активировать функцию автоматического выхода и установить временной интервал автоматического выхода из системы.

Рекомендации:

Произвести контроль установки настроек SIMATIC LOGON путем контроля конфигурационного файла:
C:\Documents and Settings***{All Users\Documents}*** \Siemens\SIMATICLogon\settings\slsettings.ini

Параметры контроля конфигурационного файла:
[Screensaver]
UseScreensaver=1 - Used SIMATIC Logon automatic logoff
WaitTime=46620 - Delay Time in Seconds
TimeToLogout=30 - Time until automatic logoff
[LogonService]
ClientWatchTimeOut=2000 - Delay Time in Seconds
Timeout4ControlClients=1000 - Delay Time in Seconds

6.2 Включено напоминание о смене пароля

При использовании приложения SIMATIC LOGON требуется активировать функцию напоминания о смене пароля. Рекомендуемое значение упоминания не должно превышать двух месяцев.

Рекомендации:
Произвести контроль установки настроек SIMATIC LOGON путем контроля конфигурационного файла C:\Documents and Settings***{All Users\Documents}***
\Siemens\SIMATICLogon\settings\slsettings.ini

Параметры контроля конфигурационного файла:
[Config]
Reminder=0 - Days for reminder of password expiration

7. SIMATIC SIEMENS WINCC (НАСТРОЙКИ ДОСТУПА)

7.1 Измененить стандартные пароли для демонстрационных учетных записей

Требуется изменить стандартные пароли для демонстрационных учетных записей WinCC:

- winccd/winccpass
- wincce/winccpass
- DMUser/Data&Pass

Рекомендации:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=45027800&caller=view

7.2 Изменить стандартный пароль администратора

Требуется изменить стандартный пароль администратора WinCC создаваемый по умолчанию:

- Administrator/Administrator

Рекомендации:
SIMATIC WinCC Explorer ->*Project Name*-> User Administrator -> *Open* -> *User* -> Change password …

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=27064342

Проверить список пользователей WinCC 7 путем выборки пользователей из базы данных запросом: SELECT * FROM ***{имя_базы}***.dbo.PW_USER

7.3 Использовать сложные пароли для учетных записей, имеющих доступ к HMI

Контролируйте сложность паролей для членов групп, имеющих права на изменение параметров системы, таких как:

- No. 1: User administration
- No. 2: Value input
- No. 3: Process controlling

Рекомендации:
SIMATIC WinCC Explorer ->*Project Name*-> User Administrator

Проверить права пользователей WinCC 7 путем выборки из базы данных запросом:
SELECT * FROM ***{имя_базы}***.dbo.PW_USER

7.4 Ограничения членства в группах управления

Контролируйте сложность паролей для членов групп, имеющих права на изменение параметров системы, таких как

- No. 1: User administration
- No. 2: Value input
- No. 3: Process controlling

Рекомендации:
SIMATIC WinCC Explorer ->*Project Name*-> User Administrator

Проверить права пользователей WinCC путем выборки из базы данных запросом:
SELECT * FROM ***{имя_базы}***.dbo.PW_USER

7.5 Отключите возможность использования локальных групп для предоставления доступа

Сервер с установленным компонентом WebNavigator может быть доступен только группам, расположенным в том же домене.

Рекомендации:
Проверить установки WinCC Web Settings -> Session Logon/Logoff - > Disable local groups of SIMATIC Logon

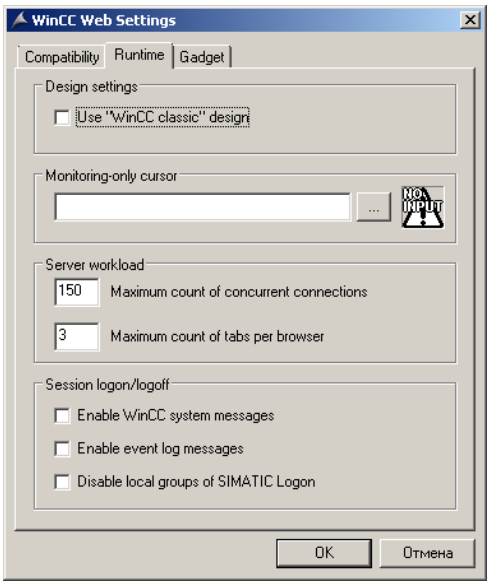
8. SIMATIC SIEMENS WINCC (ПРОТОКОЛИРОВАНИЕ)

8.1 Активируйте протоколирование событий входа в систему в журнале – архиве

Необходимо производить журналирование событий входа/выхода из WebNavigator Client (системные сообщения с номерами 1012400" или "1012401").

Рекомендации:
Проверить установки WinCC Web Settings -> Session Logon/Logoff - > Enable WinCC system messages

Доступный проект и окна для сети можно найти в файле:
C:\Program Files\Siemens\WinCC\WinCCProjects\Project\WebNavigator\PDLPublisher.xml
Настройки:
C:\Program Files\Siemens\WinCC\WinCCProjects*Project*\WebNavigator\ProjectData.xml
<variable name="WebNavigatorRT.LogSessionStartStop">1</variable>



WinCC Web Settings

8.2 Активируйте протоколирование событий входа в систему в системном журнале Windows

Необходимо производить журналирование успешных сеансов входа, используя системный журнал Windows

Рекомендации:
Проверить установки WinCC Web Settings -> Session Logon/Logoff - > Enable event log messages

Доступный проект и окна для сети можно найти в файле:
C:\Program Files\Siemens\WinCC\WinCCProjects\Project\WebNavigator\PDLPublisher.xml
Настройки:
C:\Program Files\Siemens\WinCC\WinCCProjects*Project*\WebNavigator\ProjectData.xml
<variable name="WebNavigatorRT.EventLogSessionStartStop">1</variable>

9. SIMATIC SIEMENS WINCC (КОНТРОЛЬ ПРОЕКТА)

9.1 Сконфигурированы ограничения пользовательского интерфейса

Необходимо ограничить действия, выполняемые с использованием пользовательского интерфейса Windows в среде программного обеспечения WinCC. Требуется деактивировать горячие кнопки, такие как Ctr+Alt+Del, Alt+Esc, Alt+Tab, Ctl+Esc и другие.

Рекомендации:
Для проверки состояния установки ограничений на пользовательском интерфейсе WinCC, необходимо зайти в установки WinCC Explorer -> Computer properties -> Parameters -> Disable Keys

Контроль ключей реестра:
Windows 64бит:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Siemens\WinCC\Winlogon\Permissions]
"AllowShutdown"=dword:00000001
"AllowLogout"=dword:00000001
"AllowCtlAltDel"=dword:00000001
"AllowAltEsc"=dword:00000000
"AllowAltTab"=dword:00000001
"AllowCtlEsc"=dword:00000000

Windows 32бит:
[HKEY_LOCAL_MACHINE\SOFTWARE \Siemens\WinCC\Winlogon\Permissions]
"AllowShutdown"=dword:00000001
"AllowLogout"=dword:00000001
"AllowCtlAltDel"=dword:00000001
"AllowAltEsc"=dword:00000000
"AllowAltTab"=dword:00000001
"AllowCtlEsc"=dword:00000000

9.2 Отключено использование горячих клавиш управления интерфейсом

Для каждого из проектов запрещено использование горячих клавиш управления интерфейсом.

В установках проекта WinCC должно быть отключено использование горячих клавиш для работы с окнами Windows (Alt+F4, Resize, Move, Minimize, Maximize и др.).

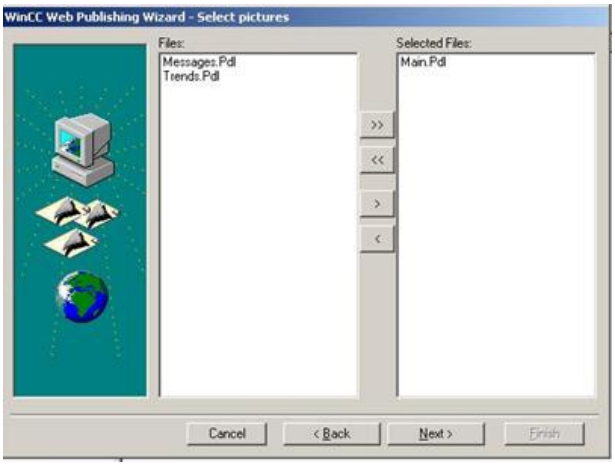
Рекомендации:
Для проверки состояния установки ограничений на пользовательском интерфейсе WinCC, необходимо зайти в установки WinCC Explorer -> Computer properties -> Graphics Runtime

10. SIMATIC SIEMENS WINCC (WEBNAVIGATOR – ПУБЛИКАЦИЯ ЭКРАНОВ)

10.1 Опубликованы только необходимые экраны

Необходимо обеспечивать контроль за экранами проекта, публикуемыми с использованием компонента WebNavigator.

Рекомендации:
Произвести контроль публикуемых экранов WinCCExplorer - > WebNavigator -> WinCC Web Publishing Wizard -> Select pictures



Публикация окон

Дополнительный материал:

Проект:
Какие проекты есть на компьютере:
C:\Documents and Settings\All Users\Документы\Siemens\WinCC\MCP.INI
[Recent File List]
File1=C:\Program Files\Siemens\WinCC\WinCCProjects\Test\Test.MCP
File2=C:\Program Files\Siemens\WinCC\WinCCProjects\Test1\Test1.MCP
File3=C:\Program Files\Siemens\WinCC\WinCCProjects\Test2\Test2.MCP

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\MCP
"a"=SZ:C:\Program Files\Siemens\WinCC\WinCCProjects\Test\Test.MCP
"b"=SZ:C:\Program Files\Siemens\WinCC\WinCCProjects\Test1\Test1.MCP
"c"=SZ:C:\Program Files\Siemens\WinCC\WinCCProjects\Test2\Test2.MCP

Последний проект:
HKEY_CURRENT_USER\Software\SIEMENS\WINCC\Control Center\Default Settings
"LastOpenPath"=SZ:C:\Program Files\Siemens\WinCC\WinCCProjects\Test\
"LastProject"=SZ:C:\Program Files\Siemens\WinCC\WinCCProjects\Test\Test.MCP

Настройка автозапуска проекта:
HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\WinCC\AutoStartWinCC
"ProjectName"=SZ:C:\Program Files\Siemens\WinCC\WinCCProjects\Test\Test.MCP

Проверка проекта:
HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\WinCC\STORAGE\PROJECTLIST
\CC_Test_1_12_12_04_16_36_45 - имя проекта и время изменения настроек
"FullPatch"=SZ:\\SERVER2\WinCC_Project_Test_1\Test_1.mcp - имя компьютера и путь к проекту
"TYPE"=SZ:Multi User - указатель что проект может использоваться по сети для доступа другим пользователям

Лицензии:
[HKEY_CURRENT_USER\SOFTWARE\SIEMENS\SWS\LicenseManager\Explorer]
"LastDrive"=sz:C:\

C:\AX NF ZZ (скрытая папка)
Файлы *.EKB

Активно используется для вывода информации о лицензиях:
HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\SWS\LicenseManager\FixedViews\5211
"Columns"=sz: возможно перечислены лицензии по внутренним номерам

Проверка состояния лицензий:
C:\Program Files\Siemens\WinCC\diagnose\LicenseLog.xml

Ссылки на материалы Siemens по безопасности SCADA систем:

SIMATIC Process Control System PCS 7 Security concept PCS 7 & WinCC (Basic):
http://support.automation.siemens.com/WW/llisapi.dll/csfetch/60119725/Main_de_Sicherheitskonzept_SIMATIC_en_en-US.pdf

Security for PC-based Automation Systems with Windows Embedded Operating Systems:
http://cache.automation.siemens.com/dnl/TU/TU2MDQ5MQAA_55390879_Tools/55390879_Security_Leitfaden_PCBased_WE_en.pdf

Исключительные права на материалы, публикуемые в настоящей документации принадлежат ЗАО «Позитив Текнолоджиз» и охраняются в соответствии с действующим законодательством РФ. Допускается цитирование и использование данных материалов в соответствии с действующим законодательством РФ и с обязательным указанием правообладателя и источника заимствования.

ЗАО «Позитив Текнолоджиз» не несет ответственности за последствия использования данных материалов или невозможности их использования, а также не несет ответственности за принятые пользователями решения на основе данных материалов и результаты, полученные в ходе принятия таких решений.