

Security for PC-based Automation Systems with Windows Embedded Operating Systems

SIMATIC PC-based Automation

Security Guidelines • October 2011

Applications & Tools

Answers for industry.

SIEMENS

Industry Automation and Drive Technologies Service & Support Portal

This article is taken from the Siemens Industry Online Support. The following link takes you directly to the download page of this document:

<http://support.automation.siemens.com/WW/view/en/55390879>

Caution

The functions and solutions described in this article confine themselves to the realization of the automation task predominantly. Please take into account furthermore that corresponding protective measures have to be taken up in the context of Industrial Security when connecting your equipment to other parts of the plant, the enterprise network or the Internet. Further information can be found under the Content-ID 50203404.

<http://support.automation.siemens.com/WW/view/en/50203404>

If you have any questions concerning this document please e-mail us to the following address:

<mailto:online-support.industry@siemens.com>

You can also actively use our Technical Forum from the Service & Support Portal regarding this subject. Add your questions, suggestions and problems and discuss them together in our strong forum community:

<http://www.siemens.com/forum-applications>



SIMATIC PC-based Automation Security for Windows Embedded Operating Systems

Security Guidelines

Industrial Security

1

**Firewall to Protect
Network Services**

2

**Access Protection for
Windows Systems**

3

**Protection against
Malware**

4

**Methods for
System Hardening**

5

**Operating System
Software Updates**

6

Internet Links

7

History

8

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.



DANGER

DANGER indicates that death or severe personal injury will result if proper precautions are not taken.



WARNING

WARNING indicates that death or severe personal injury may result if proper precautions are not taken.



CAUTION

CAUTION with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE

indicates that an unintended result or situation can occur if the relevant information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

**WARNING**

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Foreword

Purpose of the documentation

This documentation provides information and recommendations on security aspects of PC-based automation systems with Windows Embedded operating systems. The objective is to provide an overview of the basic and most important options and mechanisms.

Required knowledge

This documentation is intended for persons involved in configuring, commissioning and servicing PC-based automation systems with Windows Embedded operating systems. Basic administration knowledge and IT techniques for Microsoft Windows operating systems are required.

Validity of the documentation

This documentation is valid for the following PC-based automation components:

- SIMATIC IPC227 / IPC277
- SIMATIC IPC427 / IPC477
- SIMATIC IPC577
- SIMATIC IPC627 / IPC677
- SIMATIC S7-mEC, EC31 (embedded controller)

with the following embedded operating systems:

- Microsoft Windows Embedded Standard 2009 (WES2009)
- Microsoft Windows Embedded Standard 7 (WES7)

Table of Contents

Legal information.....	4
Foreword.....	6
Table of Contents.....	7
1 Industrial Security	8
1.1 Differences between office security and industrial security	8
1.2 Security management	8
1.3 Defense in-depth strategy	10
2 Firewall to Protect Network Services	11
2.1 Introduction.....	11
2.2 Disabling services	11
2.3 Local Windows Firewall.....	11
2.4 External firewall	12
2.5 Typical communication services of SIMATIC products.....	12
3 Access Protection for Windows Systems.....	14
3.1 Introduction.....	14
3.2 Windows user accounts	14
3.3 Security policies	14
4 Protection against Malware	15
4.1 Introduction.....	15
4.2 Use of virus scanners.....	15
4.3 Use of whitelisting software.....	17
5 Methods for System Hardening	18
5.1 Introduction.....	18
5.2 Analysis of user actions.....	18
5.3 Analysis of “routes of infection”	19
5.4 Measures for system hardening.....	19
6 Operating System Software Updates	22
6.1 Introduction.....	22
6.2 Basic update options	22
6.3 Manual update.....	24
6.4 Automatic Windows Update	24
6.5 Windows Server Update Services (WSUS)	24
7 Internet Links	25
8 History.....	25

1 Industrial Security

1.1 Differences between office security and industrial security

The security mechanisms integrated in PCs and Windows operating systems generally provide a high level of security. However, these measures are typically designed for the requirements of office environments. In industrial security, the security objectives are quite similar, but, to some extent, their priorities differ significantly. While the top priorities in office IT are typically the confidentiality and integrity of information, plant availability or operability come first in industrial security.

When selecting appropriate security measures, it must always be ensured that they provide the necessary level of protection without having any negative impact on the actual operation. In this document, the description of the measures also includes examples of possible critical effects.

1.2 Security management

General information

Security management is an integral part of an industrial security concept to address all security-relevant aspects of an automation solution – be it of a single machine, a plant section or an entire plant. As the potential threats to an automation solution change over its life cycle independently of its actual function, this is rather a security management process. The objective of this process is to achieve the necessary security level of an automation solution and to maintain it on a permanent basis.

Establishing a security management process also ensures, for example, that due to the risk analysis included in it, only appropriate countermeasures will be implemented to reduce the risks. For example, such a process could look as follows:

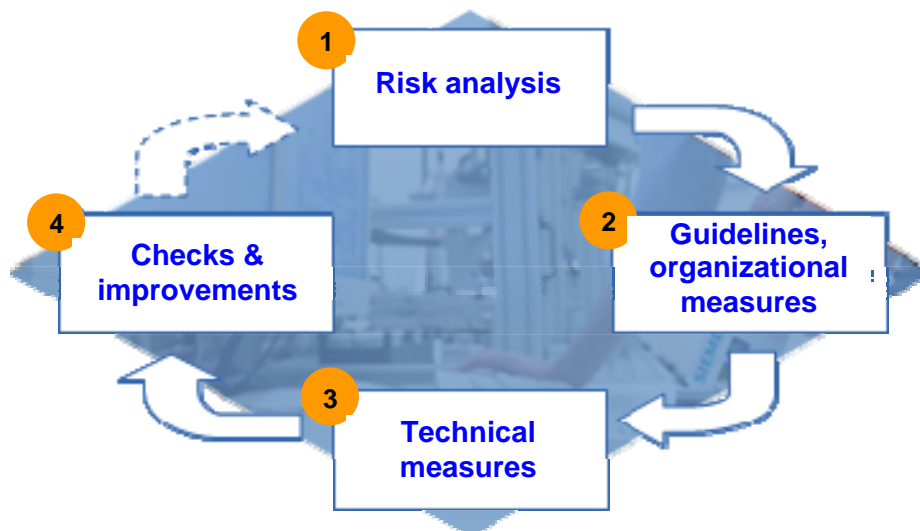


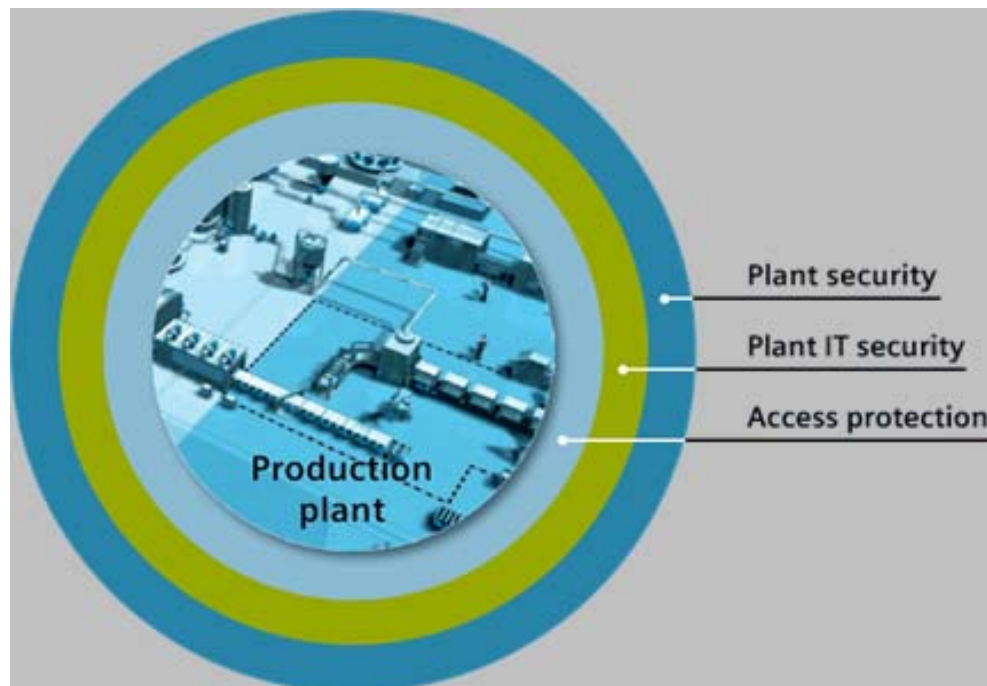
Table 1-1

No.	Step	Description
1	Risk analysis	<p>The process starts with the identification and assessment of risks of the used components, machines or plants. Based on this assessment, respective countermeasures will be taken. Examples of possible threats to PC-based automation components are:</p> <ul style="list-style-type: none"> • Infection with malware (data media, network services, downloads, ...) • Unauthorized use of operating system functions / applications • Denial-of-service effects (network overload / system overload, ...) • Spying/data manipulation
2	Guidelines, organizational measures	<p>As not all risks can be reasonably minimized by technical measures, an industrial security concept also includes organizational measures. The organizational measures include, for example, the definition of responsibilities, industrial security training or even processes to resume productive operation after security incidents.</p>
3	Technical measures	<p>Technical measures normally start with physical access or access protection mechanisms. Furthermore, they also refer, for example, to the security mechanisms of PC systems shown in this document, which are, in turn, supplemented by application-specific security mechanisms.</p>
4	Checks and improvements	<p>The final step is to check the implemented security measures to see if they work as planned. Due to the changing threats, the risk analysis should be repeated at regular intervals and the measures should be modified where necessary.</p>

1.3 Defense in-depth strategy

Typically, not all the risks of an industrial plant can be minimized by individual countermeasures. Therefore, effective industrial security concepts are normally based on a combination of several complementary countermeasures. Such a protection procedure using countermeasures that are layered and coordinated with one another is referred to as a “defense in-depth” strategy. However, such a concept does not refer to individual components, it always refers to an entire system.

In simple terms, the individual protection layers around a plant can be divided into the following groups:



Copyright © Siemens AG 2011 All rights reserved

Table 1-2

Group	Description
Plant safety	Physical protection against access by unauthorized persons
Plant IT security	Network and IT security mechanisms
Access protection	Application-specific security mechanisms

The security measures described in this document can be assigned to the plant IT security or machine IT security layer.

For more basic and detailed information on this topic, please visit the Siemens Industrial Security website listed in [Siemens Industrial Security website](#).

2 Firewall to Protect Network Services

2.1 Introduction

Many applications installed on a PC system offer their services also to the network so that they can be used, for example, from other PCs. Traditionally, this includes server services such as web servers, mail servers or FTP servers but also monitoring or remote maintenance mechanisms (e.g., remote desktop). Furthermore, such communication mechanisms are also used for mere PC-internal communication, for example between background services and applications (with GUI).

Overall, these mechanisms are very convenient, but they also involve certain risks. Each network service with security vulnerabilities is a security risk that requires an appropriate response. To generally minimize the risk, only network services that are actually required should be active or accessible via the network.

NOTICE

If the PC system can only be accessed via remote access (e.g., remote desktop, iAMT), it is particularly important to ensure that these services are not accidentally disabled or blocked.

2.2 Disabling services

The most effective protection of a network service that is not needed is to completely disable it. Basic options to disable network services can be found here:

- Direct configuration of network services, for example when they provide separate configuration user interfaces
- Indirect configuration of services via loadable engineering projects
- Services management of the Windows operating system (“Control Panel > Administrative Tools > Services > Startup Type: “Disabled””)

A detailed recommendation cannot be made as to which services should be enabled or disabled as it strongly depends on the used products and the implemented automation solution.

2.3 Local Windows Firewall

An alternative option to protect access to network services is to use local firewall software. Such a solution is particularly advantageous if the service is to be used on the local PC system or if it cannot be disabled but external access is to be blocked.

The current Windows Embedded systems already include such an integrated firewall that protects against unwanted access via the network.

You can enable Windows Firewall via the Control Panel. Make sure that you enable only network services that are to be externally accessed. You can enable or disable these settings at any time by checking or unchecking the programs or services in the exception list (“Exceptions” tab).

2.4 External firewall

In addition to the integrated firewall software of PC-based systems, there is also the option to restrict access to network services via external security components. For this purpose, security components such as SCALANCE S are used, whose firewall mechanisms can allow or block access to network services. Aside from the additional security functions of these components (e.g., VPN), the advantage of this solution is that it is independent of the actual PC system. For example, the local firewall may be affected by a malware infection while this software does not affect the external firewall.

2.5 Typical communication services of SIMATIC products

The following table provides an overview of the communication services that are typically used by SIMATIC products.

Table 2-1

SIMATIC product	Application	Service			Port
WinCC flexible RT	Web Server	Access to internal HTML pages (HTTP)			80
		Access to internal HTML pages (HTTPS / SSL)			443
	Sm@rt Server	Connection to the Sm@rtServer			5800
		Connection to the Sm@rtServer			5900
	OPC	OPC via DCOM	Server	Connection establishment	135
			Client	Communication	dyn.
		OPC via XML (client <=> server)			80
		OPC UA (binary protocol)		Communication	4840
	Archiving	Archiving on a server		UDP	137, 138
				TCP	139
	Other	Transfer via Ethernet		Configuration PC	dyn.
				Panel	2308 or 50523
		Communication between		S7 controller	102
				Panel	dyn.
		PROFINET IO communication			
E-mail (SMTP server)				25	
Modicon controller (Modicon channel MODBUS TCP/IP)				502	
Simatic Net	OPC Server	OPC-UA discovery for discovering OPC-UA server end points			4840
		SIMATIC NET OPC UA-S7 server (TCP port)			4845
		SIMATIC NET OPC UA-PNIO server (TCP port)			4847
		PROFINET CBA and OPC DCOM mode			135

2.5 Typical communication services of SIMATIC products

SIMATIC product	Application	Service	Port
		SIMATIC NET S7 OPC A&E Server	dyn.
		SIMATIC NET SIMOTION OPC A&E Server	dyn.
		SIMATIC NET SNMP OPC A&E Server	dyn.
		SIMATIC NET OPC DA Server	dyn.
		DLL hosting from remote inproc OPC server	dyn.
		ASP.NET for the OPC XML-DA IIS web service	dyn.
		SIMATIC NET PN CBA OPC server	dyn.
		NETBIOS name service for finding OPC servers (UDP)	137
		NETBIOS datagram service for finding OPC servers (UDP)	138
		OPC Enum	dyn.
	OPC Client	SIMATIC NET OPC SCOUT V10	dyn.
	Web Server	HTTP port 80 web service (TCP)	80
	PC Station	CCAgent for the remote configuration of PC stations	dyn.
		RedundancyControl for the remote configuration of PC stations	dyn.
		CCEServer for the remote configuration of the local PC station	dyn.
	S7-300/400 CPs	HTTP WebServer (TCP)	80
		SMTP (E-mail)	25
		SNMP	161, 162
		DHCP	68
		FTP	20, 21
		ISOonTCP	102
		PROFINET	135
	Other	ISO-on-TCP connections	102
		SIMATIC NET PROFINET IO	dyn.
		ICMP incoming echo request	dyn.
		SNMP (UDP)	161
		SNMP traps (UDP)	162
		PROFIdrive ProfilServer	dyn.
SIMATIC NET PROFIdrive BusServer		dyn.	
SIMATIC NET Core Server SR	dyn.		
WinAC RTX		0, 20, 21, 23, 25, 80, 102, 135, 161, 8080, 34962, 34963, 34964, 65532, 65533, 65534, 65535	

3 Access Protection for Windows Systems

3.1 Introduction

In practice, many Windows Embedded systems are used with a user account with administrative rights. This procedure may be very convenient, but it increases the security risk posed by, for example, unauthorized modifications or infections with malware.

One of the reasons for this is the fact that nearly all operations and settings on a Windows system can be made with administrator rights. This makes it possible to cancel all protection mechanisms that have been previously set up.

3.2 Windows user accounts

As with a standard operating system, an administrator account should only be used for special administrative tasks when using a Windows Embedded operating system. A user account with standard user rights should be used for regular operation.

Such a user account with limited rights can be created with the graphical user management once at least two administrators have been created.

NOTICE

Make sure that you directly assign appropriate passwords to all user accounts to avoid security vulnerabilities.

Alternatively, limited user accounts can also be managed directly via the user/group management of Computer Management. This can be done both locally and centrally via a domain controller.

3.3 Security policies

Depending on the use case, additional modifications of the security settings for the user accounts or the entire system can be made using the security policies. These security policies can be set both locally in the system and globally via domain policies.

These policies allow you to define, for example, the following features:

- Minimum password length / password complexity requirements
- Minimum / maximum password age
- Account lockout threshold / duration
- Users who may log on locally or using Remote Desktop
- Users who may shut down the system

To access the local security policies, select “Administrative Tools” in the Control Panel.

CAUTION

When using security policies, it is absolutely necessary to consider the effects on the respective automation application.

For example, when an account lockout threshold is specified, there is a risk that access to user interfaces will be denied in critical situations.

4 Protection against Malware

4.1 Introduction

As malware represents one of the biggest threats to PC-based automation systems, this risk must be appropriately addressed. The protection mechanisms described in the previous chapters provide a certain security, but there are still routes of infection that are not covered by these mechanisms. Therefore, a frequent request is to use virus scanners known from the Office environment also for PC-based automation solutions.

4.2 Use of virus scanners

General information

When using virus scanners for PC-based automation solutions, it must be considered that the availability and throughput of an automation solution have top priority. However, virus scanners require resources already in normal mode – i.e. there are no viruses – that are then not available for the automation task and therefore have to be considered when selecting the PC platform:

- **Computing power**
While scanning, virus scanners use CPU computing power. This may cause an increased base load of the PC and possibly result in longer automation processes.
- **Communication performance**
Monitoring the communication for malware may reduce the communication performance.
- **PCI bus load, jitters**
Particularly the scanning of files on the mass storage (HD, SSD, CF card) of the PC may result in a bus load on the PCI or PCIe bus that may affect access to devices for direct or distributed I/O.

The selection of the virus scanner is normally specified by the IT departments of the end customer / owner as their aim is to perform centralized maintenance for infrastructure protection and information security reasons.

The following sections provide recommendations on how to sensibly use virus scanners in an automation solution. When selecting a virus scanner product, it should be ensured that these recommendations can actually be implemented.

Updating the virus scanner

New malware appears almost daily, which spreads quickly, particularly via the Internet. Even though automation solutions are rarely connected directly to the Internet, short-term virus infection caused by devices in the plant network or data media may still occur.

Therefore, it is mandatory to regularly update the virus scanners. As a rule for the update interval, the following rule typically applies here:

Generally, the use of a virus scanner is only useful if a
cyclic virus pattern update << 14 days
is ensured.

If regular updates at this interval cannot be reliably ensured, a virus scanner should not be used as a virus scanner with obsolete virus patterns provides no real security. Instead, alternative options for system hardening such as whitelisting should rather be used.

Aside from the update cycle, the option to perform the update must also be considered:

- **Internet access:** Generally, direct Internet access will not be available for machines so that it will not be possible to use the typical automatic updates of virus scanner products.
- **Update via teleservice:** If a machine can be accessed at any time at the end customer, it can also be considered to update the automation PC via teleservice mechanisms – however, the overhead for many machines in the field is considerable and the update must normally be synchronized with production breaks at the end customer.
- **Update by the end customer:** The most sensible option is for the end customer's IT department to perform the update. Virus scanners used in enterprise environments typically support centralized distribution of pattern updates for various devices.

General settings for virus scanners

As availability and performance of the automation task are the top priorities of automation solutions, the following boundary conditions should be considered when selecting and using a virus scanner:

- **No active scan during production times** (performance, jitters)
In particular, complete scans of the PC must be postponed to times when there is no active production, for example after the last production shift, during shift change-over or general maintenance times.
- **No active scan of the communication** (performance)
This avoids delays or slowing down of, in particular Ethernet-based, communication.
- **No quarantine, deletion or automatic repair of (supposedly) infected files**
Continuous operation of the machine/plant has priority. Due to quarantine, deletion or repair attempts, the file no longer functions and the automation solution fails – it may not fail immediately, but at a later time when the file is actually needed. It may then no longer be possible to link the failure to the original malware incident. Instead, the detected infection should only be indicated.
- **Central indication of a (supposed) virus infection**
Local indication may be unfavorable for the following reasons:
 - Unattended PC systems (“headless”) do not detect these messages and countermeasures cannot be taken.

- The message indicating a virus infection eclipses the actual machine operation. This means that important contents of the visualization application may be overlooked or lost.
- This may confuse the operating staff and cause well-intentioned but harmful panic reactions, for example hard shutdown of the PC.

Therefore, indication of the virus infection should be central depending on the use case. Measures can then be assessed and initiated by qualified and trained personnel of the end customer.

- **Operation on Windows Embedded Standard systems**
For operation on Windows Embedded Standard systems (WES2009, WES7), the following must be observed:
 - Check whether the selected virus scanner is approved for operation on systems with WES2009 or WES7.
 - Virus patterns and updates should not be stored on EWF/FBWF-protected partitions or directories to ensure that they are stored permanently.
 - Alternatively, EWF/FBWF must be disabled before updating the virus patterns. When doing so, make sure that the state of the systems is secure (e.g., reboot before “EWF commit and disable”, see also “Managing EWF or FBWF in Embedded systems” in 6 Operating System Software Updates).
 - Windows Embedded Standard systems usually feature a CF card. The storage capacity must have sufficient reserve to store the updates.

Training maintenance staff at the end customer’s facility

Essentially, the requirements for using antivirus software in the automation environment differ from the requirements in the typical IT environment. Therefore, all persons involved in service and maintenance (maintenance staff, IT departments of the end customer, ...) should be familiarized with the above-listed principles and trained accordingly.

4.3 Use of whitelisting software

Whitelisting protection mechanisms ensure that only reliable programs and applications are executed on a PC system. They prevent unauthorized software from being executed and installed applications from being modified. This kind of protection is available via security applications that have to be additionally installed.

Major advantages of whitelisting technology are:

- Low resource requirements
- Protective effects without regular pattern updates
- Automatic protection against third-party program codes (e.g., via a USB flash drive)
- Increased protection against zero-day exploits
- Can be post-installed on existing systems – it is therefore particularly interesting for operating systems for which the manufacturer no longer provides updates.

5 Methods for System Hardening

5.1 Introduction

As described in the previous chapter, the use of virus scanners in automation solutions is subject to certain boundary conditions or, in some cases, cannot be reasonably implemented. Therefore, other measures have to be taken to protect the system against malware and unauthorized use.

The below-listed measures are only a small selection of possible measures. It is mandatory to identify the routes of infection. As each implementation of an automation solution is customized, the respective characteristic features have to be taken into account. Therefore, the essential steps are as follows:

1. Analysis of user actions
2. Analysis of routes of infection
3. Determination of measures

5.2 Analysis of user actions

First, it is important to analyze which persons have access to or contact with the automation solution. Typical users are:

- Operating staff
- Service and maintenance staff of the owner
- Service and maintenance staff of the OEM / machine manufacturer
- Service and maintenance staff of another company (for example, of the “neighboring machine”)
- IT employees of the end customer
- Staff from production engineering and logistics
- Unauthorized users in the machine environment

For each of these users, it has to be defined which actions are to be performed – or prevented – on a machine or which intentions these users may have. For example, this can be:

- Operation of the machine in normal mode
- Access to Windows for setup purposes, making updates
- Transfer of files for production optimization or production planning
- Online access for production optimization or production planning
- Modification/extension of the configuration (well-meant improvements – warranty!)
- Access to Windows for parasitic use, e.g. accessing the Internet (surfing the Internet during breaks), installing Office software or games
- Sabotage to create additional “breaks”

5.3 Analysis of “routes of infection”

In addition to the above-listed users and actions, intended to a greater or lesser extent, possible routes of infection for malware have to be identified:

- Via the company/plant network
 - Wired
 - WLAN
- Via teleservice accesses
- For PG connection
- Via data media
 - USB flash drive
 - USB hard drive
 - CF card / SD card
 - CD/DVD
 - RFID
 - Bluetooth
 - ...

5.4 Measures for system hardening

This section lists a number of normal measures. However, it cannot provide a complete list of all possible measures and the measures are not suitable for all possible cases. Additional measures must be determined or invented according to the above analysis and the extent of the measures must, of course, be reasonable in relation to the actual threat.

Mechanical protection of hardware interfaces

Reliable protection against infections via hardware interfaces can be established by providing mechanical protection of interfaces against unauthorized use. This includes:

- Placing the PC or programmable controller in an enclosed control cabinet
- Access protection for keyboard and mouse using locked drawers under the screen
- Blocking of unused hardware interfaces (e.g., network ports)

Disabling hardware interfaces that are not required

PC interfaces such as USB, etc. can normally be effectively disabled via software configurations, for example via:

- BIOS (only generally)
- Windows Control Panel
- Network configuration
- Additional applications

5.4 Measures for system hardening

Disabling autostart mechanisms

The AutoRun or AutoPlay function automatically executes or runs software on a removable storage medium that is connected to a PC. Malware can then be installed without any explicit user action.

The AutoRun or AutoPlay function can be disabled. For a more detailed description, please refer to the Microsoft Knowledge Base article on how to disable AutoRun.

Disabling system services that are not required

Just like network services, other system services can also be disabled to further increase system security. However, this requires that these services be no longer needed to perform the automation task or other necessary supplementary functions.

Preventing unauthorized persons from accessing Windows

Essential protection of a PC in an automation solution can also be achieved by preventing unauthorized persons from accessing the PC or by making it extremely difficult for them to access the PC. To do so, two options are available:

- Limiting user rights using Windows means.
For details, see chapter 4 “Protection against Malware”.
- Locking Windows access, for example via the HMI application.

Locking Windows access using the HMI application can, for example, look as follows:

- The PC is configured for autologin at boot and starts automatically with limited rights as configured for a machine operator.
- When booting, the HMI application starts automatically. WinCC can be configured so that no Windows access is possible until start.
- To allow Windows access for necessary maintenance work, a control element to exit the HMI application can be configured in special, password-protected maintenance screens.

Using write filters for embedded systems (EWF / FBWF)

Enhanced Write Filter (EWF) and File Based Write Filter (FBWF) allow the protection of individual partitions of the mass storage against write access. Write accesses during runtime are buffered in the RAM so that, from the software perspective, it appears as if write access was possible. However, all write accesses will be canceled when the next loss of voltage occurs or the next time the PC is shut down/rebooted so that the PC starts in the state when enabling EWF/FBWF.

- By doing so, EWF/FBWF prevents software that has been installed without authorization from remaining on the system on a permanent basis.
- However, it does not prevent the PC from infections by malware and the malware can – as long as the PC remains turned on – continue to spread from it. But as with software that has been installed without authorization, the malware will typically be removed after rebooting.
- When enabling EWF/FBWF, it must be ensured that data is not stored on partitions or directories that are not protected (EWF) or that were excluded from protection (FBWF). It is absolutely necessary to follow the documentation of the used software to see if and how data can be stored on unprotected drives or directories.

- If EWF/FBWF must be disabled for installation or configuration, the PC must first be set to a defined, secure state. By disabling EWF/FBWF using the “Commit&Disable” command, current system changes will be permanently stored. If at this time, for example, malware has infected the computer, it will be permanently stored on the mass storage because of the command. As a precaution before executing the “Commit&Disable” command, the automation PC should first be disconnected from the supply and, if necessary, removable storage media should be removed and the PC should be restarted.

Protecting hardware-based remote maintenance mechanisms (iAMT)

For devices that support hardware-based remote maintenance mechanisms such as Intel AMT, it must also be ensured that they are appropriately protected. As these mechanisms allow comprehensive access to PC systems via the network, the risk of unauthorized use exists also in this case.

If these mechanisms are not needed, they should, in the simplest case, be disabled. When using these mechanisms, you should additionally use secure access data and secure communication settings.

6 Operating System Software Updates

6.1 Introduction

From time to time, Microsoft publishes corrections of its own products in the form of patches. Some of these patches are used to increase the stability of the operating system or applications; more frequently, however, they are used to resolve security-relevant vulnerabilities before they can be exploited. However, Microsoft typically releases these patches only for the Windows Standard and Server operating systems and not for operating systems of the Embedded family.

The operating systems of the Embedded family (WES2009, WES7) are componentized operating system versions of the standard PC operating systems Windows XP and Windows 7 that are specially tailored to the respective hardware.

For industrial use, components that are not needed (e.g., Media Player, games, ...) are removed from the operating system. This is done, for example due to the reduced size of the image, to allow the use of CF cards and thereby increase robustness through non-rotating mass storage devices. In addition, special features such as EWF / FBWF are integrated that due to the reduced number of write accesses on CF cards, allow a longer service life (MTBF) of the system.

Therefore, when installing patches, only components of the operating system may be updated that are actually part of the customized operating system. Otherwise, there is a risk that the limited memory on the CF cards will be quickly exhausted by unnecessary components. Only the operating system of WES7 and higher automatically detects which patches have to be installed due to the operating system composition.

CAUTION

Before installing patches on productive systems, they always have to be checked for compatibility on suitable test systems.

Furthermore, backups should be created to be able to quickly restore productive systems in case of incompatibility.

6.2 Basic update options

General update options

The update mechanisms of standard PC operating systems (Windows XP / Windows 7) and embedded operating systems (WES2009 / WES7) do not differ in their approach.

To install patches, the following basic options are available:

- **Manual update**
Manual installation of downloaded Windows updates that are linked via Microsoft bulletins.
- **Automatic Windows Update – not for WES2009**
Automatic download of Windows Security Updates via an Internet connection to the Microsoft Windows Update server and manual installation on the devices.
- **Windows Server Update Services (WSUS)**
Targeted provision of Windows updates for all groups or specific groups of devices using a company-internal WSUS server.

CAUTION Installing patches during running operation on a productive system may result in limitations of the real-time characteristics.

Furthermore, it may be necessary to reboot the system after installing the patches. It is therefore recommended that patches only be installed during a maintenance phase of the productive system.

Characteristic features of embedded systems

Compared to standard Windows systems, certain characteristic features have to be considered when updating embedded operating systems:

- All components of the patch are installed during the update – even if they were not included in the original image. This fact must be taken into account with regard to the available memory of the CF card.
- When EWF / FBWF are used on the system, they must be disabled before installation and then be re-enabled. When doing so, it is recommended that first a reboot be performed before disabling to restore the original system state.
- When using WSUS, additional script files (WUS-FS) are necessary that automatically perform the handling with EWF / FBWF.

Tools for OEMs

In addition to the above-mentioned tools, there are a number of other Microsoft tools that support, in particular, OEMs in servicing their own images. The following tools are used to check updates and to install them in existing images:

- **Microsoft Baseline Security Analyzer (MBSA)**
Via an active Internet connection, MBSA determines the Windows Security Updates necessary for the device.
- **Package Scanner (Pkgscn)**
Determines the Windows Security Updates necessary for the device from updates that have already been downloaded.
- **Deployment Image Servicing and Management (DISM)
formerly: Package Manager (PkgMgr)**
Command-line tools for servicing Windows images (WIM files).
- **ImageX**
Provision of WIM file to capture, modify and apply file-based data media images.
- **Sysprep**
Preparation of WIM files for transfer to other computers.

These tools are not discussed in greater detail in these guidelines. For more information on these tools, please refer to the Microsoft websites.

6.3 Manual update

6.3 Manual update

When a Windows Embedded system is updated, the necessary security updates are first downloaded to any PC (with Internet access) via the Microsoft Download Center (\2\).

The necessary updates can be determined first, for example, with the aid of Microsoft Baseline Security Analyzer (MBSA).

After downloading the updates and, if necessary, transferring them to the target system with the Windows Embedded operating system, these updates that are available as separate files can be installed individually or on a script-controlled basis.

While this variant is useful for a small number of PC systems, the overhead for simultaneous update of several PCs increases rapidly.

6.4 Automatic Windows Update

In addition to manual update, the Windows update mechanism also supports automatic update. Via an Internet connection to the Microsoft Update server, there are regularly checks for new updates for the target system.

CAUTION When using this update method, automatic installation should not be used as it may affect the automation process. Instead, updates should be manually selected, downloaded and installed.

For SIMATIC PC systems, this mechanism is only available for Windows Embedded Standard 7 and higher.

6.5 Windows Server Update Services (WSUS)

General information

Especially for operating or updating a larger number of PC systems, it is recommended to use a central infrastructure for software distribution. For Windows Server operating systems, Microsoft offers Windows Server Update Services (WSUS) that allows targeted distribution of updates necessary for the client PCs. In addition, WSUS provides the option to centrally obtain updates from Microsoft and to individually assign the updates released for the respective devices in the local (company) network.

WSUS with write filter support (WUS-WF)

Generally, WSUS does not provide support for the EWF/FBWF mechanism that is common in Windows Embedded systems. As a consequence, after restarting the system – for example after installing an update –, all changes that have been made will be lost if the write filter was enabled.

In WES7, both EWF and FWBF can be automatically disabled during updating and then re-enabled via VBScript files with the aid of WUS-WF (Windows Update Servicing with Write Filter). This method can also be used to integrate additional 3rd party updates. For more information, please refer to \3\.

7 Internet Links

This list is by no means complete and only provides a selection of useful information.

Table 7-1

	Topic	Title
\1\	Siemens Industrial Security website	http://www.siemens.com/industrialsecurity
\2\	Microsoft Download Center	http://www.microsoft.com/downloads
\3\	Windows Update Servicing with Write Filter	http://msdn.microsoft.com/en-us/library/ff850921.aspx
\4\	Reference to this entry	http://support.automation.siemens.com/WW/view/en/55390879

8 History

Table 8-1

Version	Date	Modification
V1.0	10/2011	First edition