

Time for action: Support has ended for Windows 2000 in industrial automation



FIGURE 1. Windows operating systems are widely utilized in industrial automation, providing a familiar foundation for a human-machine interface (HMI)

Microsoft stopped issuing extended support and security updates for Windows 2000 in July 2010. What are the implications for your industrial network?

Torsten Rössel
Inninate Security Technologies
AG

All good things come to an end. And so it is with Microsoft® extended support and security updates for Windows 2000®, which ended in July 2010. Any manufacturer with industrial applications that are based on Windows 2000 may wisely be considering a newer operating system in order to remain in production with the necessary security support. But migrating to a new operating system can be time-consuming, disruptive and expensive.

Are there any better alternatives? This article presents several proven solutions.

Microsoft Windows operating sys-

tems are widely used for networked industrial automation equipment. Unfortunately, these industrial Windows applications, like their counterparts in office networks, are also vulnerable to known and emerging Windows security loopholes that continue to be discovered and exploited. Microsoft's Lifecycle Policy for business and developer products provides five years of Mainstream Support and five years of Extended Support, during which time necessary security updates are provided (for a total of ten years of coverage).

However, the lifetime of industrial machinery and other capital equipment is often 20 years or more of useful operation. The much shorter lifecycle of the software (in terms of ongoing protection against potential security breaches) suggests that it will usually not survive as long as the equipment it serves.

The mainstream support portion of the product offering for Windows 2000 ended in June 2005. In July 2010, the extended support for Windows 2000 also expired. Planned obsolescence is a key element of software product management and marketing. There are several historical examples.

While Windows 2000 has enjoyed a

10-year run, other earlier operating systems did not. For example, support for Windows 95 expired in December 2001. Support for Windows NT 4.0 expired after eight years in June 2004. And support for Windows 98 expired in July 2006. Common sense, good business judgment and IT security policies dictate planning ahead to anticipate the demise of current operating system software support.

What should be done?

Continuing "business as usual" with both eyes firmly shut is not a recommended course of action. Worms, viruses, Trojans, and hacker exploits are problems that cannot be ignored. The widespread popularity of Microsoft operating systems has made them an all-too-appealing target for malware creators.

In 2008, Microsoft issued 36 security updates relevant to Windows 2000, including 19 classified as "Critical," the company's highest classification. Another 16 security updates were classified as "Important." Then in 2009, Microsoft released an even-larger number of security updates — 48 for the nine year-old system, 31 of them deemed "Critical" and 16 deemed "Important!" In fact, in every month of



FIGURE 2. Industrial PCs and embedded components based on Windows Operating Systems are widely used in industrial automation and chemical process environments

2009, at least one additional breed of malware had to be dealt with by a new version of the Microsoft Windows Malicious Software Removal Tool, which was distributed with the other monthly system updates.

The notorious Conficker worm proved to be a particularly troublesome issue, as well as the dangerous and versatile Trojans, Waledac and the Bredolab downloader, ushering in a plethora of evil malware and spyware from servers hosted mostly in Russia and China. In mid-2010, the Stuxnet worm was discovered, exposing new vulnerabilities and further raising the stakes. The near future will see SCADA exploits based on Stuxnet copycats. The expiration of support for Windows 2000 means the end of available and automated security updates against these kinds of threats.

Expensive upgrades

An obvious solution, of course, is to implement an upgrade to a newer operating system that maintains current support. But such upgrades are costly. New licenses must be purchased and new software installed. And new ver-

sions of Windows tend to require the acquisition of new hardware and infrastructure, as well.

Efforts to switch operating systems can also bring unanticipated consequences involving considerable extra work and expense. For instance, certified systems and automated manufacturing processes typically require an expensive approval process when altering any of their components. Such interruptions can lead to production complications — which have a greater impact than interruptions to an office environment — and thus significant expenses can quickly accumulate associated with any upgrade.

It is difficult to calculate the potential security risks and the risks of unforeseen glitches that could affect production. The responsibility of triggering a potential cost avalanche trembles in the balance. For this reason, common sense and demonstrated logic often guide plant personnel to be ruled by the philosophy “if it’s not broke, let’s not ‘fix’ it.”

Distributed security appliances

What virtually all software security

risks share in common is that they are based on the weaknesses and vulnerabilities of network protocols and services. Hacker exploits and malware take advantage of these weaknesses over an IP-based network to gain access, control, and opportunities to create damage and enable proliferation. If security updates against newly discovered vulnerabilities are no longer available, there is an increased risk to the unsupported system, which must continue to communicate with other network nodes and with portions of the outside world (for instance, engineering and programming consultants, remote maintenance services, and so on). The days of being able to maintain a truly isolated production network are rapidly disappearing. But while vital system interconnections are obviously impossible to eliminate, many other types of potential network communications can be blocked as a way to reduce the risk of infections.

The purpose of firewalls is to control and selectively filter unrestricted Ethernet and IP-based communications on the network. In addition to front office firewalls, there are industrial network security appliances that are needed to provide “defense-in depth” — a common approach that relies on the use of numerous layers of firewalls — on the factory floor. This method of protection is better, faster, more cost-effective than IT network solutions and easily installed by plant technicians rather than IT network administrators. Such devices come in various industrial-rated formats, encompassing DIN-rail mounting, 19-in. rack mounting in cabinets, as PCI cards or as dongle-style patch cords for roaming technicians.

In “stealth mode,” these security devices are completely invisible on the network, automatically assuming the Ethernet and Internet address of the equipment to which they are connected, so that no additional addresses are required for the management of the network devices. No changes need to be made to the network configuration of the existing systems involved. The devices operate invisibly and transparently, monitoring and filtering traffic to the protected systems by providing a so-called stateful packet

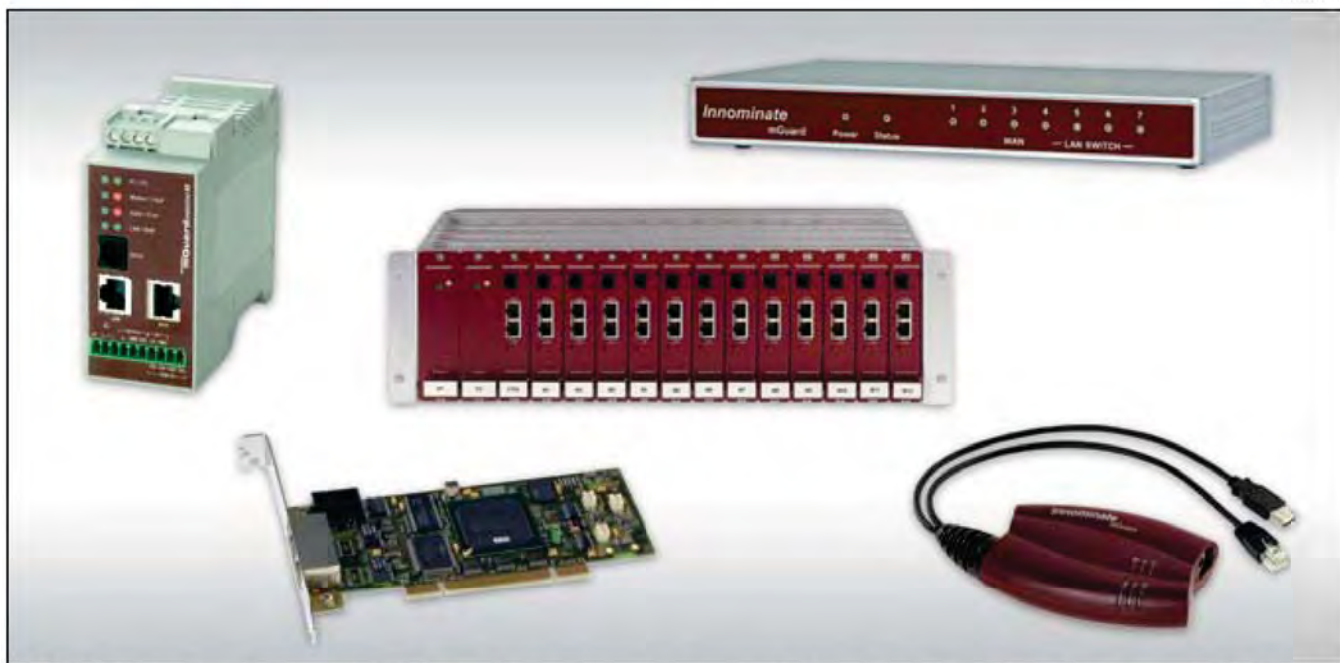


FIGURE 3. In various forms, distributed security appliances can protect Windows operating systems that are used in industrial automation. They segment the network, providing router and firewall protection, inspecting and discarding unauthorized packets, and restricting access via encrypted VPN tunnels

inspection firewall (one that is used in advanced firewalls and can recognize and discard unauthorized packets), according to rules configured via templates from a centrally located server. And with bi-directional wire speed capability, appliances will not add any perceptible bottlenecks or latency to a 100 Mb/s Ethernet network.

If required, the security of networked equipment may be further enhanced. For instance, user-specific firewall rules can be configured to restrict the type and duration of access to authorized individuals, who may login and authenticate themselves from varying locations, PCs, and Internet protocol (IP) addresses.

Virtual Private Network (VPN) functions provide for secure authentication of remote stations, and enable the encryption of data traffic.

Common Internet File System (CIFS) integrity monitoring functionality protects Windows file systems against unexpected modifications of executable code by Stuxnet-like malware, for instance. Common Internet File System / Server Message Blocks (CIFS/SMB) are the protocols behind Windows file sharing. Customers in the automotive industry and others

have already used these systems with excellent results in providing security for older production systems using Windows 95, Windows 98 and Windows NT.

Security for non-patchable equipment

There is always a substantial concern that a reckless, blanket implementation of software patches and security updates — without extensive (and expensive) certification tests prior to implementation — could inadvertently affect the operation, stability or quality of production. Thus “If it isn’t broken, don’t fix it” is often the prevailing principle in production and chemical process operations.

In the face of costs associated with certification and risks of warranty claims against machinery and equipment suppliers, many embedded PC systems are routinely operated without software patches and security updates. When this happens, these systems are essentially treated as “non-patchable” — long before the end of their Extended Support coverage from the operating system supplier. Such non-patchable systems can be protected with enhanced security using the same method of retrofitting Stealth Mode security appliances to

them, as described above.

The Stuxnet worm demonstrated that the risk of disruption and outright sabotage of industrial automation and SCADA systems is real. And the clock is ticking. Untold numbers of Windows 2000 systems no longer have access to Microsoft’s Extended Support and Security Updates, because they ended in July 2010. The time for leisurely analysis and evaluation of alternatives, decision making, planning, preparation and implementation of a new operating system has passed. Fortunately today, proven security products are available to provide immediate protection for industrial networks. These are transparent, do not affect production, and are easily implemented by technicians rather than network managers. ■

Edited by Suzanne Shelley



FIGURE 4. Industrial network-security appliances have been widely and successfully used as a simple retrofit to protect automotive-production machinery and processes that use the older Windows 95, Windows 98 and Windows NT operating systems

1. Microsoft® and Windows 2000® are registered trademarks of Microsoft; mGuard® is a registered trademark of Innominate Security Technologies AG

2. For more information about current threats to networked industrial equipment, a comprehensive 18-page White Paper entitled "Hacking the Industrial Network" (including footnotes, live Internet research links and detailed references) is available for download at www.innominate.com. An accessible discussion of "Post-Stuxnet Industrial Security" is also available.

References

1. Microsoft Support Lifecycle; <http://support.microsoft.com/lifecycle/>
2. Microsoft Security Bulletin Search; <http://www.microsoft.com/technet/security/current.aspx>
3. The Microsoft Windows Malicious Software Removal Tool; <http://support.microsoft.com/kb/890830/en-us>

Author



Torsten Rössel is the director of business development for Innominate Security Technologies AG in Berlin (Rudower Chaussee 13, D-12489 Berlin, Germany; Phone: +49-30-921028-0; Fax: +49-30-921028-020; Email: troessel@innominate.com; www.innominate.com).

He is a frequent speaker at industry conferences and is the author of numerous articles on the protection of networked industrial systems and secured remote services for machinery over the Internet. Rössel was educated in mathematics and computer science at the Technical University of Karlsruhe and graduated with a diploma in mathematics.