# Looking into Windows

## Windows XP has reached the end of its life – what are the implications?

VOLKER JUNG, ANTHONY BYATT – Microsoft's successful and very popular Windows XP operating system is now well over a decade old. While about 30 percent of Windows users worldwide still rely on XP, an operating system as old as this cannot be supported forever. Accordingly, Microsoft ceased XP support on April 8th, 2014. This means there are no new security updates, no new patches and no active support. The effect of this is that XP will slowly become unsecure, unreliable and incompatible with most newly released IT hardware, such as PCs, PC components, network equipment and printers. In other words, the end of the XP era is affecting many industrial applications and requires a proactive response from users.

At one time, the idea of running an industrial application using Microsoft Windows would not have been entertained. However, when Microsoft introduced their Windows XP operating system over a decade ago, industry sat up and took notice. Windows XP provided the stability, flexibility and functionality needed by many industrial users and soon appeared in every imaginable type of application.

However, all good things come to an end: On April 8th, 2014 the Windows XP era concluded when Microsoft support for the product ceased. Of course, Microsoft had given ample notice and companies had been preparing for the switch for some years. Yet many questions had to be answered: Could a standalone XP system continue to run unaffected? What would happen if the XP system was integrated into another system? Would new hardware be needed and what would be the cost of this across the entire organization? What would the budget for the switch likely to be? Could virtualization fix the problem? What support would be available to migrate over onto a new system?

**Title picture**
Microsoft support for Windows XP ceased on April 8th, 2014. What are the implications for industrial users?

The answers to these questions were not always straightforward and easy, and it became clear that there were indeed significant issues raised by the end of XP support. The most significant issues can be grouped into four major categories:

- Security
- Compliance
- Lack of independent software vendor support
- Hardware manufacturer support

Of these, security issues are the most critical.

## Windows XP security updates

In 2010, the Stuxnet worm made headlines around the world. With a size of just 500 kB, this malicious software attacked at least 14 industrial sites in Iran, including a uranium-enrichment plant. Stuxnet attacked in three phases: First, it targeted Microsoft Windows machines and networks, then it sought out software (also Windows-based) used to program industrial control systems and finally it insinuated itself into the programmable logic controllers used to control machinery.

Since Stuxnet, the target-rich landscape of industrial IT has been under a sustained assault that has grown ever more sophisticated. For example, the so-called watering hole strategy has been devised as a way to introduce malware into the target systems. In this strategy, the malicious party guesses or observes which websites the company often uses, then they infect it and sit back and wait for the victim to visit the site and unwittingly download malware onto their computer. This strategic Web compromise (SWC) tactic catches victims unawares because the infected websites have previously been trusted.

An intruder can manipulate authentic user profiles on a system to allow outsiders access.

Further, an intruder can manipulate authentic user profiles on a system to allow outsiders access. PC configurations can also be manipulated and PCs can then, for example, become the homes of remote access trojans (RATs) – malware programs that give an intruder administrative control over the target computer. RATs can be infiltrated into a PC via an email attachment.

1 Control/HMI (human-machine interface) systems to be evolved

| System/HMI | Comment |
|---|---|
| System 800xA | 800xA core systems<br>(V5.0 and older) |
| Freelance | Freelance systems (V6.2 – V9.1) |
| Power Generation Portal/Tenore | All Windows-based versions |
| Conductor NT | All Windows-based versions; count is number of servers, not number of systems |
| Process Portal B | All versions |

Once the host system is compromised, the intruder may use it to distribute more RATs to form a botnet – a collection of compromised computers that are manipulated in concert to cause further disruption.

Because a RAT enables administrative control, it allows the intruder to monitor user behavior through keyloggers or other spyware; activate a webcam; access confidential information; format drives; delete or alter files; and so on.

In June 2014, the Havex malware family made headlines by attacking control systems in different branches of industry, including the energy sector. A RAT is a main component of Havex. The RAT trojanized websites of industrial control system (ICS) and supervisory control and data acquisition (SCADA) manufacturers. In total, 146 servers were attacked by Havex; 88 variants of the Havex RAT were used; and 1500 IP addresses were traced in an attempt to identify victims. Clearly, Havex represented a serious attack on industry.

In July 2014, the “energetic bear” virus infected over 1,000 energy firms in Europe and the United States. This virus theoretically allows hackers to take control of power plants.

2 XP upgrade strategies

| Windows XP | | Controller | | | Windows 7 | Windows 8.1 |
|---|---|---|---|---|---|---|
| 800xA | 3.1<br>4.0<br>4.1<br>5.0 | All | → | 800xA | 5.1 | 6.0 |
| Freelance | 6.2<br>7.1<br>7.2<br>8.1<br>8.2<br>9.1 | All | → | Freelance | 2013 | 2015 |
| Conductor NT | All | DCI | → | 800xA | 5.1 | 6.0 |
| | | Freelance | → | Freelance | 2013 | 2015 |
| | | | → | 800xA | 5.1 | 6.0 |
| | | Harmony | → | 800xA | 5.1 | 6.0 |
| | | | → | Symphony + | 2.0 | |
| PPB | All | MOD 300 | → | 800xA | 5.1 | 6.0 |
| | | Freelance | → | Freelance | 2013 | 2015 |
| | | | → | 800xA | 5.1 | 6.0 |
| | | Harmony | → | 800xA | 5.1 | 6.0 |
| | | | → | Symphony + | 2.0 | |
| PGP/Tenore | All | Freelance | → | Freelance | 2013 | 2015 |
| | | | → | 800xA | 5.1 | 6.0 |
| | | Harmony | → | 800xA | 5.1 | 6.0 |
| | | | → | Symphony + | 2.0 | |

From these examples it is apparent that the industrial IT environment is quite vulnerable enough – and without critical Windows XP security updates, PCs are wide open to attack by viruses, spyware and other malicious software that can steal or damage business data and information. Antivirus software no longer provides full protection for XP systems. Any devices remaining with XP can be used by attackers as an entry point into IT networks. This means that even computers running supported operating systems can then also be compromised.

## Hardware

Most manufacturers of PC hardware, printers and network equipment have already stopped supporting Windows XP on new hardware. This means that the software drivers required to run Windows XP on such new hardware are, in most cases, no longer available – ie, there will be no XP drivers for new hard disks, printers, graphic cards, network equipment, etc. Buying a replacement XP computer will not be easy or cheap. XP-based hardware will become obsolete and hard to find. Unplanned shutdowns caused by unavailability of hardware components will become more frequent.

## Compliance

Businesses that are governed by regulatory obligations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, may find that they are no longer able to satisfy compliance requirements if they remain with Windows XP. With so much personal and private data now stored on servers, data security is a very significant concern.

## Lack of independent software vendor support

Many software vendors no longer support their products that run on Windows XP as they are unable to receive Windows XP updates. For example, the new Microsoft Office package takes advantage of the newest Windows and does not run on Windows XP.

## What to do

With so many issues to be overcome, what course of action should be taken? The recommendation made by Microsoft and all cyber security companies is to upgrade to Windows 7 or 8. This includes distributed control system vendors with control systems running operating systems with Windows XP and older ➔ 1 – 2.

Of course, an evaluation can be made of the cost of keeping XP installations safe versus upgrade costs. Remaining with Windows XP is a high-maintenance undertaking and requires tools and support from experienced cyber security companies. Some of the actions that need to be undertaken include:

- Reduce the size of the registry to include only those services that are absolutely needed.
- Utilize domain name server (DNS) sinkholes to block access to the real website.
- Issue an alert when an endpoint-initiated remote desktop or virtual network connection is detected.
- Prevent binary execution for temporary users in the file system or issue an alert when this occurs.
- Whitelist service binaries in the operating system.
- Issue an alert for service starts/stops/changes.
- Audit access control lists, etc.
- Make regular control system backups.
- Buy a stock of compatible IT parts.

Retaining Windows XP is becoming untenable. It is an inevitable part of industrial IT life that an evolutionary software step has to be taken every so often and the move upwards from Windows XP is one of the more significant of these. The move will put users in a position where they are well placed to meet the security, hardware, software and compliance demands of the modern industrial IT world.

ABB strongly recommends that customers running Windows XP operating systems evaluate their system life-cycle plans and risk mitigation strategy. Simultaneously, ABB is offering solutions that can remedy or mitigate risks and help customers better protect their plants and personnel while ensuring safe operations and continuous production. Services are available to help meet the needs of every customer – including customers who are unable to upgrade immediately and those who elect to remain on Windows XP.

**Volker Jung**
Process Automation Division
Mannheim, Germany
volker.jung@de.abb.com

**Anthony Byatt**
Editorial consultant
Louth Village, Ireland