OCTOBER 2013

PHOENIX CONTACT
INSPIRING INNOVATIONS

WIN XP – Don't Get Left Behind

By Eric Reichert
Product Marketing Specialist – Industrial PCs and HMIs
Phoenix Contact USA

Abstract

When Chaucer said that all good things must come to an end, he undoubtedly was not referring to Windows XP's end of life. However, as XP has just passed 12 years of existence, there are plenty of IT directors and CIOs that would still claim the parallel exists, since support is scheduled to end in April 2014.

As punny as the topic can be portrayed, the sunset of such a beloved operating system is not humorous to those who standardized. With its departure, current users will lose their continued support, inclusive of security patches, hotfixes, and bug fixes, which kept everything running smoothly. Licensed computers might soon be portrayed as potential vulnerabilities and threats to the processes and applications that they control, which in turn could lead to a mass exodus of XP users. Since data from Net Applications, a web analytics firm, shows that 31.6 percent of users are still on this platform as of October 2013,[1] the topic is fuming with speculation as to whether or not corporations should make the switch and whether or not this end of life (EOL) is of concern to them. While no one expects that come April 9, they will walk into their factories and experience immediate downtime and attacks, those that have standardized on the platform realize that the threat is imminent nonetheless. Leading up to this event, there will be both those making the argument for the upgrade, as well as those opposing it. This white paper will highlight both schools of thought and the role a supplier could play in either scenario.

CONTENTS

Afflicted users

Since customers that have industrial PCs need to manage multiple lifecycles when maintaining their systems, they have to ensure that drivers are up-to-date based on chipset revisions, hard drives aren't nearing end of life, and many other subtleties that could ultimately lead to downtime during their process. A particular worry is the security holes that can develop in their system when it is attached to a public network. Contrary to a private network, where computers aren't connected to the outside world via the Internet, public networks are vulnerable to hackers and viruses. These kinds of vulnerabilities are what causes administrators to apply security patches and take additional measures, such as the Phoenix Contact mGuard security device, to ensure their cyber security. However, in order for security patches to be released, the operating system needs to still be under support by Microsoft.

Back in 2002, Microsoft released a Support Lifecycle policy that offered more transparency to its end consumers. The policy stated that Windows products would receive a minimum of 10 years of support, with five years mainstream and the other five extended support. Due to this transparency, customers could plan accordingly and upgrade their systems to the successor, allowing them to receive security patches on the upgraded system.

Based upon the aforementioned data, some would argue that only computers connected to the outside world (i.e., the Internet) would be afflicted and be candidates for change. However, even networks not attached to the Internet run the risk of being exploited remotely. In the case of Windows XP, best practice is to switch to a succeeding version such as Win 7 or Win 8.

Since Microsoft notes that the average enterprise deployment can take 18 to 32 months, urgency depends upon the potential risk XP users are willing to endure. For users on networks connected to the Internet, the urgency to beat the April 8 deadline is formidable. For customers that need to make the switch but are unable to by April 8, certain suppliers have the ability to still sell licenses after the April 8 deadline, but there will still be no patches/support. The extension should also allow companies that are late on their switch to allocate the funding and resources.

Two trains of thought

It's not broken, so don't fix it

To those that find XP's end of life a moot point due to an "if it's not broken, don't fix it" mentality, realize that by not taking action, you are preventing future action. If your company abides by a Kaizen strategy, where there is momentum toward continual improvement, realize that changing the computer image could be an extremely sensitive matter, as you would need to ensure that you don't expose yourself to new vulnerabilities and threats. Presumably, most users that would continue to use XP after the EOL would not be on an open network subject to outside threats, but if that were to ever change, there would be an imminent threat of attacks.

A new theme within the control segment is this exact concept, known as future-proofing, where a company makes decisions today that could potentially impact decisions a few years from now. While this theme could more easily be exhibited with a computer feature, such as multi-touch, it is still just as applicable with operating systems. However, we understand that continual improvement isn't necessarily a key performance indicator, and there are costs, support, and uncertainty paired with such an upgrade. The question at that point becomes whether or not the current stability outweighs the future potential of added functionality, efficiencies and long-term cost savings.

Two trains of thought *(continued)*

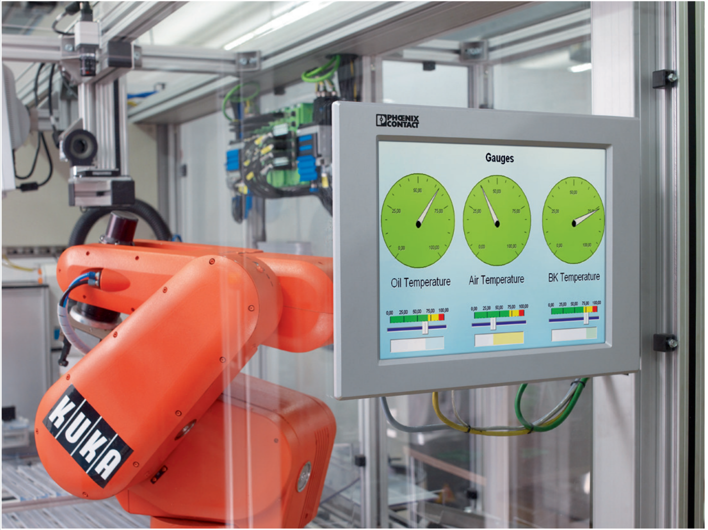

Figure 1: Up to 37.2 percent of industrial PC users are still running Windows XP. Now is the time to plan ahead and start future-proofing your industrial PC.

While some would argue that attackers would spend their time focusing on systems representative of the majority of users, according to Net Applications, WIN XP users still represent a staggering 31.6 percent of users as of October 2013. While the United States only has 16.2% still using this platform, other prominent countries in the tech world, such as China, have a gut-wrenching 72.1 percent. Assuming that these numbers are considerable enough for attackers worldwide, it is only a matter of time before vulnerabilities are discovered. (Figure 1)

One might ask how they are discovered so quickly. It is actually in part by the work produced by the Microsoft Security Response Center (MSRC). Although seemingly backwards, since the MSRC's intention is to secure the systems they support, each release of an update leads the way for hackers to discover where they should focus their efforts next.

Since MSRC patches both reactively and proactively, each update is an opportunity for attackers to reverse-engineer the fixes to see where potential vulnerabilities once were. Due to the fact that unsupported platforms never received the packages, the reverse engineering allows an entryway into all systems that have passed their security update sunset.

While the obvious solution might be to upgrade to a newer operating system, sometimes one simply can't, due to the significant costs and interruptions. Software upgrades within an operating production network commonly encounter unintended and unanticipated consequences.

Another viable alternative solution is to use distributed security appliances, such as those based on Phoenix Contact's mGuard technology. Those hardware firewalls/routers protect non-patchable legacy systems on the network. In addition, they can be easily installed by plant-floor technicians without interrupting production, plus they can be configured and launched from a central server console. The resulting advantage is a low-cost hardening of these systems by a simple and transparent installation of plug-and-play modules wherever required.

With mGuard CIFS Integrity Monitoring, Phoenix Contact offers an industry-suitable solution to protect Windows-based automation components against malware and malicious attacks. To achieve this, mGuard Integrity Monitoring supervises file systems against unexpected modifications or additions to programs, dynamic link libraries, and other executable code without utilizing virus patterns – thus eliminating the need for their permanent update. This innovation can even detect damages from zero-day exploits for which virus patterns don't even exist yet. (Figure 2)

Two trains of thought *(continued)*

Figure 2: If users choose not to upgrade to a new OS, a distributed security device, such as the FL mGuard, can provide some protection. mGuard's CIFS Integrity Monitoring can even detect damages from zero-day exploits for which virus patterns don't even exist yet.

Who, how, what, when, where!

The second school of thought does not deal with whether or not a corporation should make the switch, but rather how they will perform the switch. While the majority of this plan needs to be based on a case-by-case basis, there are several common underlying rules that companies can follow to best structure their switch.

First and foremost, they should make sure that the supplier they are using to convert their units is able to offer WIN XP licenses past the sunset date. Since it takes nearly a year and a half for most corporations to make the switch, they would want to make sure that in the interim there are still methods to fulfill their current business model until everything is set in place for the upgraded units. Otherwise, on top of the upgrade expenses there would be additional opportunity cost from the lost business.

When everything is in place for the upgrade process to begin, it makes the most sense to outline a schedule for the implementation of upgraded units. This schedule will be contingent upon how many units can be installed in any given week. This number should be conservative, as it doesn't make sense to have units sitting on the shelf. Only under extreme circumstances would a customer want to purchase the units up front, they might need to make additional changes that were unbeknownst until that moment. It's also important to note that industrial PCs generally have limited warranties, so in order to receive the maximum warranty they would need to be put into use immediately.

By staging the implementation and purchasing through a supplier with extended license support, companies are able to control a situation that easily could have become volatile without the proper attention to detail.

Conclusion

Now is the time to plan ahead and to start future-proofing your industrial PC. Without extended support or a feasible downgrade path, you can potentially expose your IPC – and worse yet, your entire business – to security risks that far outweigh the cost of an OS upgrade. If your IPC hardware is no longer state-of-the-art, it might make sense to replace the outdated hardware with a new, better-performing, energy-efficient IPC, switch to a newer OS, and upgrade your security system with the latest mGuard technology. Not only will the new hardware enhance productivity, it will also safeguard you from unwanted downtime due to security breaches.

References:

1. Net Applications, *"Realtime Web Analytics With no Sampling."* NetMarketShare.com. October 16, 2013. <http://netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>

ABOUT PHOENIX CONTACT

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 50 international subsidiaries, including Phoenix Contact USA in Middletown, Pa.

For more information about Phoenix Contact or its products, visit www.phoenixcontact.com, call technical service at 800-322-3225 or e-mail info@phoenixcon.com.