Technology Introduction

Standardization of Windows PC System for Inspection

OGISO Shigetoshi

1 Introduction

KYB internally fabricates its inspection devices to be used for internal production inspections because the critical inspections during production processes are packed with the company's abundant knowhow. Among them are a shock absorber (hereinafter "SA") performance inspection system and SA appearance inspection system using image processing. With a necessity of high-speed processing of mass data, these inspections use personal computer (PC) systems. However, inexpensive PCs for office automation (OA) applications are remodeled at an interval as short as six months to two years. This has troubled the company since the same model of PC as the previous one was not available to be used for addition or replacement in the case of a failure.

With this background, KYB developed inspection systems running on an operating system (OS) for embedded systems Note 1) for use in industrial PCs that were available over the long term. The developed systems had been used since the internal fabrication in 2007. However, the software vendor's support service for Windows® Note 2) XP Embedded (XPE), which was the OS for embedded system Windows® XP on which the developed systems ran, was terminated in 2014.

These inspection systems were connected to a communication network to enable production data collection and central control, as well as remote maintenance services. Once the software support service was terminated, however, the vendor was supposed to no longer release new security patches or other measures to fix any serious security holes in the OS. The inspection systems might even be unable to be online depending on the type of the security holes detected. In this case somebody would have to struggle to directly collect data from all the PCs online. In addition, the systems could not provide remote maintenance services any more, resulting in delayed responses to any failures. Thus there arose the urgent need to reestablish an inspection system running on another OS.

Moreover, the production of PC parts was terminated as well. There also arose a need to update the hardware to a new configuration.

Besides the systems described above, some other inspection systems compatible with earlier PC versions were being operated. These systems also needed to be updated in the near future.

The situation made KYB develop a standardized Windows® PC based inspection system.

Note 1) Operating system (OS) for measuring equipment, automatic teller machines (ATMs) or vending machines, not for office equipment or computer servers.

Note 2) Windows is a registered trademark or trademark of Microsoft Corporation in the United States and other countries.

2 Specifications

The basic specifications are shown in Table 1.

Year by year, the image processing technology required for appearance inspection, in general, has increased in degree of difficulty, and the related processing operations have become more and more complicated. To catch up with the changes, the basic specifications of PCs have been enhanced with higher CPU processing speed and higher main memory capacity.

Table 1 Basic specifications

	Conventional PC system	New PC system	
	For SA performance inspection and image processing	For SA performance inspection	For image processing
OS	Windows® XP Embedded (32bit)	Windows® Embedded Standard7 (64bit)	
CPU	Intel® PentiumM Intel® Core2Duo	Intel® Corei7 (3th) 1.7GHz Note 3)	
Main memory	512MB	2GB	4GB
Bus standard	CompactPCI	PCI	PCI Express PCI
C Drive capacity	1GB	8GB	16GB
Security software	N/A	Whitelist	

Note 3) PentiumM, Core2Duo and Core i7 are registered trademarks or trademarks of Intel Corporation in the United States and other countries.

The conventional bus used CompactPCI compatible with Peripheral Component Interconnect (PCI). The CompactPCI standard features high resistance to vibration and contact failures. This standard was originally introduced because the PC systems of two earlier generations had had frequent faults due to poor contacts in the board. However, the market share of the CompactPCI standard was likely to drop, posing uncertainty about future parts supply. KYB then decided to introduce the PCI bus, which is still the mainstream, because of the substantially improved quality of recent boards. Most other similar in-house systems also used the PCI bus, proving no compatibility problems. The introduction of the PCI bus brought another benefit where the system update can be shared with similar in-house systems. A faster PCI standard called PCI Express was needed to achieve higher-speed transfer of image data from cameras.

3 Features of the System

This chapter describes four features of the renewed system.

3.1 Compatibility

An important point of the development was to maintain compatibility with conventional systems.

SA performance inspection system has long been introduced in large numbers both outside and inside Japan. On the contrary to the long life of expensive mechanical inspection equipment, the electronics-based PC system has a shorter life and has to be updated periodically. Thus, maintaining compatibility with the conventional systems of about 20 years ago remains a challenge, and achieving efficient part replacement remains an important issue. In the image processor, compatibility between the internally developed inspection software and cameras actually used is a key issue.

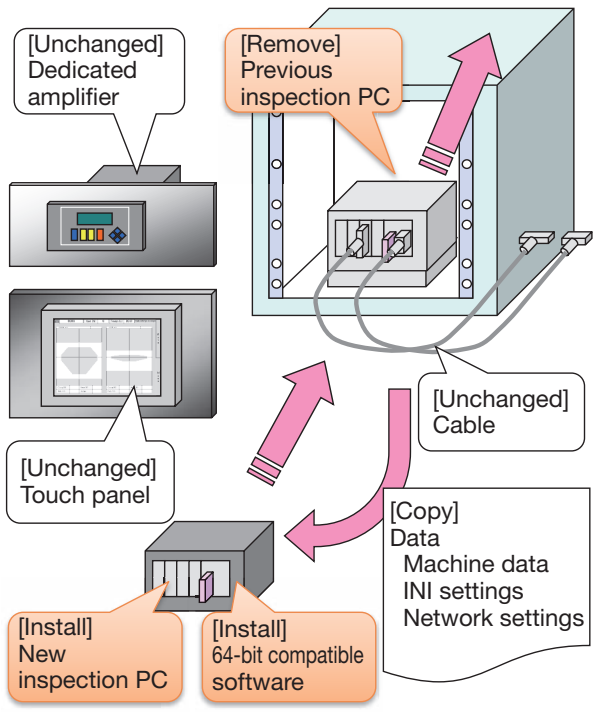

Fig.1 Compatibility for system update

The following gives a concrete example of SA inspection system compatibility. Fig. 1 shows a case in which an inspection PC of the previous generation is replaced with a new PC.

The PC is connected with the following three major devices:

① Dedicated amplifier
② Touch panel
③ Sequencer (Only the cable is shown in Fig. 1).

For replacement, the previous inspection PC is removed and replaced with a new inspection PC that has been already set up. The new PC is connected online with the peripheral equipment unchanged. The conventional 32-bit type inspection software is updated to a 64-bit compatible version. The machine data used for setting the inspection standard and setting files are just copied to the new system as they can be shared between the two systems.

These setup tasks as well as operation verification have already been actually conducted on line, confirming proper operation.

For the systems from two generations back that use a monitor-integrated PC, a touch panel needs to be added. Converter cables are available to support any peripheral equipment with different types of connectors. In this way the system can be updated at a low additional cost.

3.2 Robustness

To maintain software/hardware compatibility, it is a precondition to use Windows® OS. Furthermore, to implement a robust OS for embedded systems, KYB selected Windows® Embedded Standard7 (WES7) designed for Windows® 7 that had been proven in the company at the time of development in 2014. The image processor was changed from the conventional 32-bit type to a 64-bit compatible unit in order to support input of high-volume image data.

WES7 features the recovery of the previous state in a power cycle after a setting change. In other words, the storage area of the system, including the OS is write-protected. If you change the settings normally, new settings will be written in a virtual drive, which will be erased when the power is turned off. The system will be next started up from the original drive. To write a new setting, you must use a special command after inputting the new settings. This design allows the system to be restored in a power cycle, even if the data is lost in the case of power failure or infected with malware Note 4).

Robustness has been checked with several systems already running, verifying that no problem has occurred since the introduction.

Note 4) Generic name for a variety of forms of malicious software programs including computer viruses, worms and Trojan horses.

3.3 Security Measures

Even OSs for embedded systems need security software because they may be infected with malware during operation. In general, security software needs to

periodically update its virus definition files. However, it is impossible for the systems used in some of KYB's overseas sites not connected to the network to automatically update the definition files. The systems, even if connected to the network, may have OS failure during update of the definition files in the case of power failure or inadvertent shutdown due to an operating error, which may directly lead to a halt in the production line. Therefore, KYB uses security software that does not require updates for use in OSs for embedded systems.

Security software can roughly be divided into two types: blacklisting and whitelisting. This system uses whitelist security software.

Both types have a list of files in advance and check each application software program against the list before start-up to determine whether to permit or reject the start-up of the program. These security software programs behave differently as they operate in accordance to their permit system:

(1) Blacklisting

Based on the list of malicious programs, start-up of any applicable programs is prohibited.

(2) Whitelisting

Based on the list of safe programs (those existing in the PC), only start-up of whitelisted programs is permitted.

Specifically, the two types of security software behave as indicated in Table 2. The blacklist type permits the OS to fully work and application programs to be updated while the whitelist type prohibits all updates. For malware control, the blacklist type may fail to reject unknown malware while the whitelist type is able to prohibit the start-up of all programs including malware.

Therefore, it is generally said that the whitelist security software is better for industrial applications.

In fact, KYB checked with the security software vendor through an infection risk survey that the whitelist security software was effective in protecting systems from even the notorious ransomware [Note 5)] Wanna Cryptor, which caused a large-scale worldwide infection in May 2017.

Other technologies including Firewall and User Account Control (UAC) are also combined with the security software to protect the system.

Note 5) Type of malware that encrypts data in the victim's PC and requires the victim to pay ransom in exchange for a password.

Table 2 Blacklist and whitelist security programs

		Blacklist	Whitelist
OS	Start-up	○	○
	Update	○	×
Application	Start-up	○	○
	Update	○	×
Known malware	Activate	×	×
Unknown malware	Activate	△	×

○: Yes ×: No △: Unclear

3.4 Automated Set-Up

The developed system has been installed into several PCs by several departments every year. The installation procedure normally includes setting of numerous parameters for networking, and security and installation of driver software programs for peripheral equipment along with customization. These tasks are likely to be done erroneously if carried out by humans. The whole procedure needs man-hours of around half a day to a whole day for full manual work.

KYB then constructed an automatic installer to allow anybody to establish a PC system with the same quality level in a short time.

The following describes how the installer has been constructed to automate the set-up.

First, the standard WES7 development kit was used to build an installation function for key components of the OS, including disk configuration and user accounts. Next, an installer for the drivers provided by the vendors who released the peripherals was prepared. The installation was automated by combining the installer with a software program with which you can program keyboard typing and mouse operation according to instructions shown on the screen during installation. Finally, a batch file [Note 6)] was created to automate the sequential installation and setting of Windows® parameters.

In practice, Windows® XP and later OSs have stricter security. Specifically they are designed to require human approval in order to allow software installation or function change, which makes automation difficult. That is why the set-up sequence was decided by finding favorable timing for setting up with no need for approval, which eventually consumed of a lot of man-hours. This issue should be taken into consideration in future development.

The developed automatic installer was then used to carry out set-up, verifying that the installation procedure, except preparation, was completed quickly in a time as short as about 30 minutes.

Note 6) File containing OS operating commands in the order of execution. The batch file can also be executed itself.

4 System Maintenance

Thanks to simplified PC system installation, several departments now have more and more employees capable of setting up the system. Therefore the necessity of establishing a scheme of sharing the latest versions of installer, instruction manual and fault information has arisen. Instead of the conventional in-house network that enables distribution of the latest versions by file sharing, the web system has been introduced to facilitate the security enhancement.

Using the existing in-house web server, the web site shown in Fig. 2 has been developed to establish an information sharing system. The right of access to the web site is only provided to the departments concerned.

5 In Closing

PC-based production facilities are not so common and their percentage is very low. Around 15 years ago, system management from development to maintenance was sometimes covered by only two employees, which was very hard work. In spite of difficulties with system management, PC-based production facilities are indispensable to product quality. Since the departments involved in plant operation came to understand this issue, the facilities have been introduced and put into service in many production sites, both home and abroad, under the initiative of the departments concerned. I would like to take this opportunity to extend my gratitude to those involved in the introduction and operations.

I am committed to continue making efforts to bring the system even nearer to perfection in order to meet the needs of the sites.

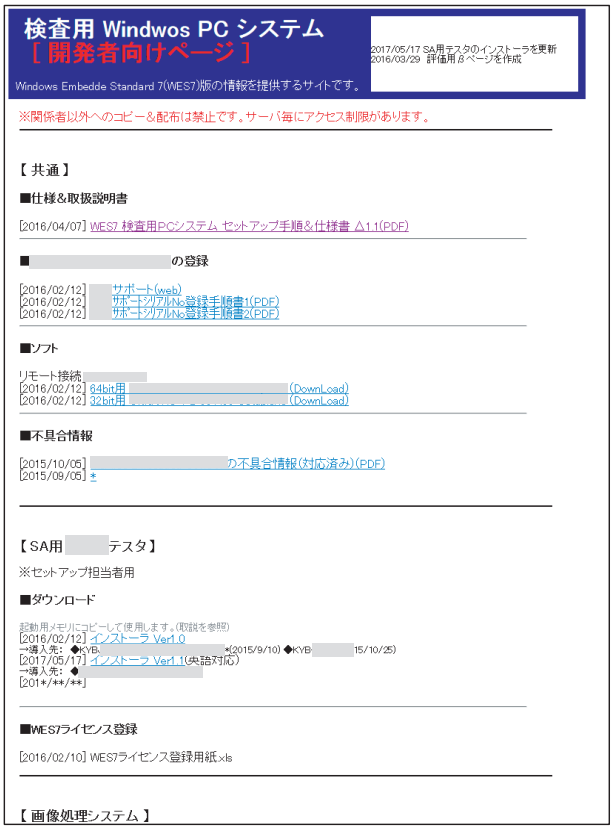

Fig. 2 In-house web site

Author

OGISO Shigetoshi

Joined the company in 1991.
R&D Sect. No.2, Production Technology R&D Center, Engineering Div.
Mainly engaged in research & development of image processing technology.