TabletPCs in Industrial Applications

White Paper

Revision A

Last Revision November 10, 2003

Invensys Systems, Inc.

Invensys Systems, Inc.
33 Commercial Street
Foxboro, MA 02035
(949) 727-3200
http://www.wonderware.com

Trademarks

CHAPTER 1

Introduction

For many years Wonderware has advocated the importance of plant intelligence, of enabling users with the right information in the right format anywhere, anytime. It is thus no surprise that over the years we have been keeping our eye on technologies that line up with this strategy. Wonderware was the first company to explore the use of the Internet in process automation, to introduce support for terminal server-based thin client technology and to explore the use of wireless PDAs for remote monitoring of automated processes.

A recent phenomenon that has caught Wonderware's attention is the TabletPC. Tablet computers, pen computing, wireless networks and character and voice recognition are not new technologies. As a matter of fact, they have been evolving for a number of years. Tablet computers, although not obvious to the public eye, have been used in many niche markets such as utilities, warehouses, public safety and emergency response systems for at least the last ten years. Some type of wireless network has existed for some time, although mostly in expensive, limited use formats. Pen computing has been around for at least a decade (Microsoft introduced its "Pen Services 1.0" in 1991, and a number of pen solutions based on other operating systems have been around too). Mobile computers have existed in the form of notebook and laptop computers for many years. But years of research, development and field experience in all of these areas (along with other related advances; for instance, lower power CPUs; lower weight, higher capacity battery technology; increased computing power; USB; Plug and Play; and advances in LCD technology) have resulted in affordable, mature technologies that have converged at a common place in time.

The introduction of TabletPCs based on Microsoft's Windows XP Tablet edition with digital ink and improved character and voice recognition, and the rapid adoption of standard Wireless LAN technology – thanks to the IEEE 802.11 specification – are some of the factors that have given the concept of mobile pen computing a new meaning.

What's more, the accumulated years of experience in the manufacture of reliable, ruggedized, industrial grade tablet computers and the use of spread spectrum technology in 802.11 wireless networks to reduce electric noise and interference opened the door for the use of industrial Wireless TabletPCs as part of industrial automation solutions.

Benefits

The increased mobility inherent in a Wireless TabletPC provides users with tremendous flexibility, enabling them to access information at the point of highest efficiency – *where they need it* – and at the time of highest efficiency – *when they need it*.

Immediate availability of Industrial Intelligence at the fingertips results in increased productivity, responsiveness and return on investment.

Industrial TabletPCs

An important consideration when selecting a TabletPC for use in an industrial application is its ability to withstand the environment it will be exposed to. Protection against particles, chemicals, humidity, wide temperature variations, liquid spills, vibration, shock and electromagnetic interference should be a strong factor in selecting the right solution.

Fortunately, Tablet Computers have been around in demanding environments associated with specific vertical applications for many years. High quality, reliable, industrial grade, ruggedized TabletPCs with well-proven records and NEMA, IP and military ratings are available in the market.

802.11 Wireless Networks

The introduction of the IEEE 802.11 standard specification, the decreasing cost of 802.11 devices and ease of setup have resulted in very rapid introduction and adoption of wireless networks at an impressive growth rate.

However, unlike other technologies where industry and large corporations are first to adopt the technology, setup infrastructures and promote its use in the general public, it has been residential users and small businesses that have been at the forefront of the Wi-Fi revolution. Affordability, ease of use and the clear benefits of the technology have attracted the general public to its adoption. Thousands of wireless network “Hot Spots” have sprung up all over the world at restaurants, shopping malls, hotels, convention centers, college campuses, airports, parks and even on intercontinental flights. Wi-Fi’s success has been such that laptop and notebook computers are being shipped with built-in wireless LAN capabilities.

Industry is also witnessing the introduction of 802.11-compliant technology in many applications such as materials handling, remote monitoring, sensors, transducers and more.

802.11a,b and g

The first wireless products that showed up in the market were compliant with the 802.11b spec, which defines the use of wireless networks in the 2.4 GHz band with up to 11 Mbps transmission capabilities[1]. To date, the largest installed base corresponds precisely to 802.11b devices.

802.11a equipment soon followed 802.11b devices. 802.11a defines the specification for wireless networks in the 5 GHz band with transmission rates of up to 54 Mbps. However, although 802.11a offers higher bandwidth and a frequency band away from 2.4 GHz phones and other common devices, its adoption has been affected by 802.11a devices' inability to connect to 802.11b equipment and, to a much lesser extent, its shorter coverage range.

802.11g was introduced as a response, extending the capabilities in the 2.4 GHz frequency band. 802.11g applies to the 2.4 GHz band with 54 Mbps and is compatible with 802.11b devices.

Security of wireless networks

As mentioned before, the ease of setup has been a key factor in the adoption of wireless networks by the general public. Manufacturers of wireless Access Points (APs) catering to home and small business users focused on making it easy for users to set up a wireless LAN. They have succeeded in doing this, making it almost a plug and play type of setup. However, in order to do this, they ship these units with security features off, enabling a totally open network and leaving it to the user to enable security and to tighten their setup.

Recent studies estimate that almost half of all home users use the default settings for their Access Points, including administrator name and password, SSID (network name), SSID broadcast enabled, DHCP enabled*, WEP security off and number of users set to maximum. It is no surprise that many home and small business users have uninvited, rogue guests on their Wireless LANs.

These studies have created the perception that wireless networks are not secure. Setting up a wireless Access Point and leaving all security settings off, though, is no different than buying a car and leaving the doors unlocked with the keys in the ignition.

[1] Actual bandwidth is a result of a number of factors, including distance from Access Point. Connection speed drops as client device moves away from Access Point.

Can wireless networks be secured?

It is a known fact that no matter how tightly you secure a network (wired or wireless), determined hackers will not stop in their attempts to breach security. The idea then is to make it as difficult as possible; and just like wired networks, you can make a wireless network as secure as you desire.

You can use the basic built-in security features of a Wireless Access Point to provide a degree of protection to your connection as well as employ more sophisticated technologies to further secure your network – such as Virtual Private Networks (VPN).

Following are a number of suggestions you could consider to secure your network if appropriate and practical to your organization:

- **Plan the coverage of your Access Point.** When possible, plan coverage of the area of interest to extend from the AP to the external walls and windows. Locating an AP near an external wall extends your coverage outside your facilities where strangers could have access to it.
- **Change the SSID (Network ID) from the default.**
- **Disable SSID broadcasting.** Broadcasting advertises the availability of your network, identifying it by name. An obvious name can make your network a target over other available networks.
- **Change administrator password from default.** This prevents intruders from tampering with your settings.
- **Enable WEP security.** Although not perfect, this deters all but the most dedicated hackers.
- **Use the highest level of WEP encryption available in your AP.** Prefer 128-bit encryption over 64-bit encryption.
- **Change the encryption key periodically.**
- **Limit the number of connections.** For example, if you only need to support five machines on an Access Point, set the maximum to 5. If you attempt to connect and are denied the connection, this may be an indication that an unauthorized computer has gained access to your Wi-Fi network.
- **Disable DHCP and use fixed IP addresses.** [2] This increases the difficulty for a potential intruder to gain access to your network by not providing an IP address automatically. (Only practical in small networks.)
- **Use MAC Filtering.** It is possible to configure an Access Point to accept connections only from devices whose MAC address belongs to an access list. (Only practical in networks with few wireless devices).

[2] Access Points that are also wireless routers for home or small business use typically provide DCHP server capabilities. Access Points for larger systems work with the corporation's infrastructure. Using fixed IP addresses may be practical in small networks only.

- **Use Firewalls.**
- **Use Virtual Private Network technology.** This is a well-proven secure technology used by many corporations to provide remote access to private networks. Today, VPNs are the most secure way to connect via a wireless network.

A number of vendors have implemented extended capabilities for authentication over wireless networks, taking advantage of Extended Authentication Protocol (EAP). Contact your vendor for more information.

Wireless networks, electric noise and interference

When thinking about the implementation of wireless networks on the factory floor, you should take into account electrical noise and interference. Electrical machinery, electric and electronic equipment as well as transmitters of various types abound in the industrial environment.

Fortunately, 802.11 devices employ Spread Spectrum techniques to make them less susceptible to electrical noise and interference. In simple terms, Spread Spectrum modulation spreads a signal in a preset pattern – known to both transmitter and receiver – over a range of frequencies. The two main Spread Spectrum techniques are known as “Direct Sequence Spread Spectrum” (DSSS) and “Frequency Hopping Spread Spectrum” (FHSS).

When considering your environment you should remember that 802.11b products share the 2.4 GHz frequency band with other common devices such as cordless phones while 802.11a devices are in the 5.4 GHz band.

Since the amount and nature of electrical noise and interference varies from site to site, we recommend that you test the selected wireless equipment in your unique environment.

APPENDIX A

Glossary of Terms

802.11

A set of IEEE standard specifications for Wireless LAN connectivity.

802.11a

Based on the 802.11 IEEE specification for Wireless LANs and ratified in 1999, it includes an amendment for high speed connectivity over the 5 GHz band. Devices designed after the 802.11a specification can provide up to 54 Mbps connectivity.

802.11b

Based on the 802.11 IEEE specification for Wireless LANs, it includes an amendment for high speed extension in the 2.4 GHz band. Devices supporting the 802.11b spec can provide up to 11 Mbps connectivity. 802.11b devices are not compatible with 802.11a. The 802.11b specification was ratified in 1999.

802.11g

Based on the 802.11 IEEE standard, 802.11g introduces an amendment for Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band. Devices supporting 802.11g can connect to devices supporting 802.11a.

Access Point

An interface that acts as a connection point between a wireless network and a wired network or that acts as a central connection point in an all-wireless network.

AdHoc

A peer-to-peer mode of operation between wireless devices without the use of Access Points (see IBSS). The alternate mode of connection is the Infrastructure mode.

BSSS

Basic Service Set network. A combination of 802.11 compliant Access Points and related infrastructure that comprise a connected wireless network. This type of network is often referred to as an ‘infrastructure’ network

DSSS

Direct Sequence Spread Spectrum. A radio transmission method that spreads its signal over a wide frequency band. See Spread Spectrum.

EAP

Extensible Authentication Protocol. An authentication protocol that supports multiple authentication mechanisms. Originally developed for use with PPP (Point-to-Point Protocol) for remote access user authentication, it is also in use with IEEE 802. EAP is also a critical technology component of Virtual Private Networks (VPN).

FHSS

Frequency Hoping Spread Spectrum. A radio transmission method in which both transmitter and receiver hop frequencies in synchronization. See Spread Spectrum.

IBSS

Independent Basic Service Set network. An 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an 'ad-hoc' network. It allows communications between stations without the use of access points.

SSID

Service Set Identifier. A unique wireless network identifier used as a password by wireless stations to gain access to a network. This SSID is attached to packets sent over the wireless network. Access Points have the ability to broadcast their SSID. Specifying an SSID ensures connection to the correct network rather than another wireless network within range. An SSID is also referred to as ESSID.

Spread Spectrum

A radio transmission method used to improve tolerance to electric interference by spreading the data signal over a band of frequencies.

ISM bands

Industrial, Scientific and Medicine bands. The group of radio frequency bands that the FCC has set aside for those uses. The ISM bands are located in the 902 MHz, 2.4 GHz and 5.7 GHz. The FCC has approved the use of wireless networks using frequencies within these bands without requiring a license.

VPN

Virtual Private Network. A technology that provides a secure tunnel to a private network over a public network (such as the Internet). VPNs can also be used in wireless networks as a means to further secure a network.

WEP

Wired Equivalent Privacy (WEP). An optional security mechanism defined in the IEEE 802.11 standard designed to offer frame transmission privacy similar to a wired network. WEP privacy is based on secret shared encryption keys used by both transmitter and receiver stations.

WPA

Wi-Fi Protected Access™. This emerging standard is comprised of a set of security mechanisms based on the 802.11i draft specification, aimed at enhancing wireless network security.

Wi-Fi

Wireless Fidelity. A generic term coined to describe wireless network technology and products following the IEEE 802.11 specification.