ABCM Symposium Series in Mechatronics - Vol. 3 - pp.659-668

AN ANALYSIS OF WIRELESS TECHNOLOGY IN MANUFACTURING SYSTEMS AND ITS DEPLOYMENT ON THE SHOP-FLOOR

Claiton de Oliveira
Department of Mechanical Engineering
School of Engineering of São Carlos
University of São Paulo, São Carlos, SP, Brazil
claiton@sc.usp.br

Jandira Guenka Palma
Department of Computation
State University of Londrina, Londrina, PR, Brazil
jgpalma@uel.br

Rafael Henrique Palma Lima
Department of Production Engineering
School of Engineering of São Carlos
University of São Paulo, São Carlos, SP, Brazil
rhlima@sc.usp.br

Arthur José Vieira Porto
Department of Mechanical Engineering
School of Engineering of São Carlos
University of São Paulo, São Carlos, SP, Brazil
ajvporto@sc.usp.br

Abstract. *The automatic shop-floor data collection aided by monitoring and supervision systems, adds precision and control improvements into decision-making process. Such improvements stimulate more and more the introduction of new technologies into the productive process. In this context, wireless technology is poised to advance shop management's ability to control and monitor shop events as they occur. As wireless technology can add a significant degree of independence in a shop's operation, workers can access part and process specifications from locations where wired networks are impractical. Hence, adding wireless capability on the shop-floor, it is possible to increase shop efficiency and employee productivity, besides being proper to constant shop-floor layout changes. Thus, this paper presents an analysis of wireless technology in manufacturing systems and its deployment on the shop-floor followed by results from an industrial case study.*

Keywords: *shop-floor management, distributed manufacturing, wireless technology, computer networks*

1. INTRODUCTION

The automatic shop-floor data collection aided by monitoring and supervision systems, adds precision and control improvements into decision-making process. Such improvements stimulate more and more the introduction of new technologies into the productive process. Nevertheless, the capturing and collection of information on the shop-floor becomes a bottleneck as data processing is no longer an issue of concern with the rapid improvement in computational and communication power (Brewer, 1999).

Without up-to-date information, it is impossible to make accurate shop-floor decisions, no matter how advanced Enterprise Resource Planning systems and manufacturing equipment are. With the introduction of radio frequency identification wireless manufacturing technologies, collection and synchronization of real-time shop-floor data become automatic or semi-automatic, improving the data reliability and reducing the cost induced from defective data (Huang, 2007).

In this context, wireless technology is poised to advance shop management's ability to control and monitor shop events as they occur. As wireless technology can add a significant degree of independence in a shop's operation, workers can access part and process specifications from locations where wired networks are impractical. Thus, adding wireless capability on the shop-floor, it is possible to increase shop efficiency and employee productivity. Besides, it is possible to simplify installation, eliminate cabling, and make machine tools mobile with wireless networking. In addition, there is no need for re-running cable when CNC machines are moved, which is proper to constant shop-floor layout changes.

This paper presents an analysis of wireless technology in manufacturing systems and its deployment on the shop-floor taking into account the technology characteristics, device features and applications as well as their advantages and disadvantages. The analysis is based on questions about security aspects, cost and integration of wireless nodes into existing wired network systems. In order to check the main issues that affect the implementation and utilization of wireless networks on the shop-floor, the proposed questions were applied to an industrial case study. In accordance with the obtained reponses, a wireless network was deployed, tested and the results reported.

The remainder of this paper is divided as follows: section 2 describes a general overview of the wireless technology. The wireless in manufacturing systems is described in section 3. Section 4 describes aspects concerning the deployment on the shop-floor. Section 5 discusses an industrial case study and finally section 6 presents the conclusions.

2. WIRELESS TECHNOLOGY

Wireless technologies represent a rapidly emerging area of growth and importance for providing ubiquitous access to the network for all of their users. Home users, students and professionals increasingly want un-tethered network access from general-purpose rooms, meeting rooms, auditoriums, and even the hallways of all kinds of buildings. Recently, industry has made significant progress in resolving some constraints to the widespread adoption of wireless technologies. Some of the constraints have included disparate standards, low bandwidth, and high infrastructure and service cost.

Wireless technologies can both support the user needs and provide cost-effective solutions. This way, wireless is being adopted for many new applications: to connect computers, to allow remote monitoring and data acquisition, to provide access control and security, and to provide a solution for environments where wires may not be the best solution. What follows is an overview of existing wireless technologies and related issues.

2.1 Communication medium

As wired communications utilize physical conductor (copper or optic fiber) connecting the transmitter and receiver to transmit information from one place (or places) to another (or others) electrically, wireless utilize electromagnetic waves as the communication medium. Thus, wireless communication involves radio frequency communication, microwave communication, and infrared short-range communication to maintain communication channels between its devices.

2.2 Communication mode

Devices in a wireless network are set up to either communicate indirectly through a central place or directly, one to the other. The first is called “Infrastructure Mode”, which requires one or more base stations or access points where all communication will be intermediated. The other is called “Ad Hoc Mode”, which does not require any access points, once user devices communicate directly with each other in a peer-to-peer manner, as shown in the Fig. 1.

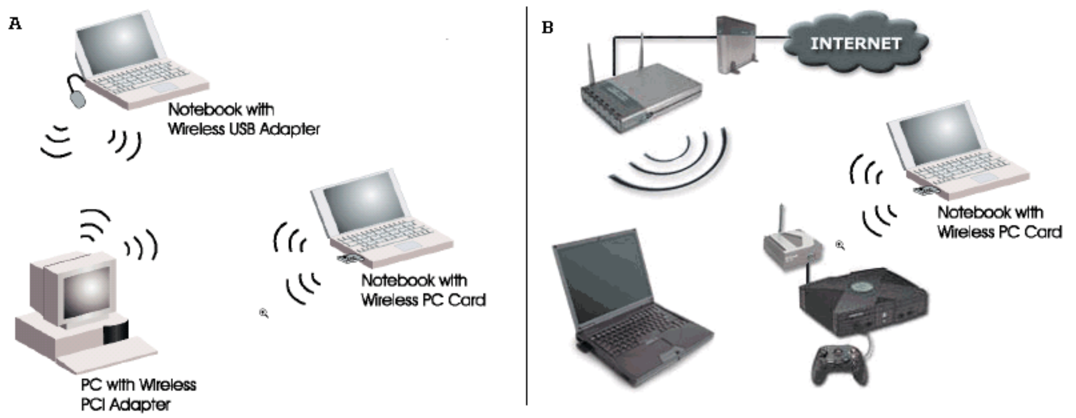

Figure 1. Typical configuration of a wireless network: A) Ad Hoc Mode and B) Infrastructure Mode

Since there is no need to purchase or install access points, ad hoc mode involves cost savings and rapid setup time. Regarding the question of performance, in an ad hoc WLAN (Wireless Local Area Network) can be higher than in a infrastructure WLAN because of no need for packets to travel through an access point. Nevertheless, this assumes a relatively small number of users, otherwise the amount of interference for all computers will increase, since each one is trying to use the same frequency channel. Therefore, for a larger enterprise where there is a strong need to access applications and servers on a wired network, it is required the use of multiple access points to separate users onto non-overlapping channels to reduce medium access contention and collisions (Tse, 2005).

2.3 Wireless local area networks

Wireless Local Area Networks (WLAN) are implemented as an extension to wired LANs within a building and can provide the final few meters of connectivity between a wired network and the mobile user. WLAN configurations vary from simple, independent, peer-to-peer connections between a set of PCs, to more complex, intra-building infrastructure networks.

WLANs are based on the IEEE 802.11 standard, which in 1997, the IEEE released as the first internationally sanctioned standard for wireless LANs, defining 1 and 2 Mbps speeds. In September 1999, they ratified the 802.11b "High Rate" amendment to the standard, which added two higher speeds (5.5 and 11 Mbps) to 802.11, operating in the unlicensed industrial, scientific and medical (ISM) band at 2.4 GHz. The basic architecture, features and services of 802.11b are defined by the original 802.11 standard, with changes made only to the physical layer. These changes result in higher data rates and more robust connectivity (Crow, 1997).

2.4 Bluetooth

Bluetooth is a technology specification for small form factor, low-cost, short-range wireless links between mobile PCs, mobile phones, and other portable handheld devices, and connectivity to the Internet. Bluetooth enables electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets. Each device can simultaneously communicate with up to seven other devices within a single piconet. Each device can also belong to several piconets simultaneously. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

A fundamental Bluetooth wireless technology strength is the ability to simultaneously handle both data and voice transmissions. This enables users to enjoy variety of innovative solutions such as a hands-free headset for voice calls, printing and fax capabilities, and synchronizing PDA, laptop, and mobile phone applications to name a few.

Bluetooth operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, with data rate up to 3 Mbps. The operating range depends on the device class, varying between 10 an 30 meters in most common mobile devices, and between 10 and 100 meters primarily in industrial use cases (Tse, 2005).

2.5 Wireless devices

To setup a wireless network depends on what the scale of the network will be. Nevertheless, the basic wireless devices required are the access point and the wireless network interface card (NIC), as follows:

- **Access Point (AP):** This piece of hardware acts as a bridge between the wired network and wireless devices. It allows multiple devices to connect through it to gain access to the network. An AP can also act as a router; a means by which the data transmission can be extended and passed from one access point to another.

- **Wireless Network Interface Card (NIC):** A wireless network card is required on each device on a wireless network. A laptop usually has an expansion (PCMCIA) slot which the network card would fit in to. A desktop computer would need an internal card Ű which will usually have a small antenna or an external antenna on it. These antennas are optional on most equipment and they help to increase the signal on the card.

These two basic wireless devices, which are shown in Fig. 2, allow communication between plenty of mobile devices, such as: laptops, notebooks, tablets, PDA's, smartphones, 3G cards, etc.

Figure 2. Two basic wireless devices: A) Access Point and B) Wireless Network Interface Card

2.6 Wireless important issues

As with any relatively new technology, there are many issues that affect implementation and utilization of wireless networks. There are both common and specific issues depending on the type of wireless network. Some of the common factors include electromagnetic interference and physical obstacles that limit coverage of wireless networks, while others are more specific, such as standards, data security, throughput, easiness of use, etc.

2.7 Wireless coverage

An important issue for wireless technology is coverage. Coverage mainly depends on the output power of the transmitter (wireless card or access point), its location and frequency used to transmit data. For example, lower frequencies are more forgiving when it comes to physical obstacles (walls, stairways, etc.), while high frequencies require clear line of sight. For each particular application, throughput decreases as distance from the transmitter or access point increases.

2.8 Wireless security

Data security is a major issue for wireless due to the nature of the transmission mechanism (electromagnetic signals passing through the air). In WLANs, authentication and encryption provide data security. Current implementations include:

1. MAC address-based access lists on access points, where only registered and recognized MAC addresses are accepted and allowed to join the network.
2. A closed wireless system, where users have to know non-advertised the network name to be able to join.
3. RADIUS server based authentication, where users are authenticated against a centralized RADIUS server based on their MAC address or their username and password.
4. Wireless Equivalent Privacy (WEP), a security protocol specifically designed for securing WLANs, which utilizes data encryption with 40-bit or 128-bit keys that are hidden from users. WEP provides three options, depending on the level of security needed: no encryption of data, combination of encrypted and non-encrypted data, and forced data encryption.

3. WIRELESS IN MANUFACTURING SYSTEMS

The automatic shop-floor data collection aided by monitoring and supervision systems, adds precision and control improvements into decision-making process. Such improvements stimulate more and more the introduction of new technologies into the productive process. In this context, wireless technology is poised to advance shop management's ability to control and monitor shop events as they occur. As wireless technology can add a significant degree of independence in a shop's operation, workers can access part and process specifications from locations where wired networks are impractical. Thus, adding wireless capability on the shop-floor, it is possible to increase shop efficiency and employee productivity, besides being proper to constant shop-floor layout changes.

3.1 Common shop-Floor problems

The capturing and collection of information on the shop-floor becomes a bottleneck as data processing is no longer an issue of concern with the rapid improvement in computational and communication power. Manual systems of data collection and capturing are time consuming, prone to errors, and tedious. It is a daunting task to trace and track work-in-progress items in a large manufacturing plant, especially when product variety is high and manufacturing layout is typically functional. Operators are busy with activities which add value to the product whereas they are hardly motivated to type in the data about their operations since such data entry operations are non-value adding activities. As a result, the information does not accurately and promptly reflect the situations and changes of the situations due to disturbances. Without up-to-date information, it is impossible to make accurate shop-floor decisions, no matter how advanced Enterprise Resource Planning systems and manufacturing equipment are. With the introduction of radio frequency identification wireless manufacturing technologies, collection and synchronization of real-time shop-floor data become automatic or semi-automatic, improving the data reliability and reducing the cost induced from defective data (Huang, 2007).

3.2 Wireless on the shop-floor

Both the introduction of computer numerical control (CNC) machines and direct numerical control (DNC) networking or communication, radically changed the manufacturing industry. Since the CNC machine controllers are capable of executing programs stored in their available memory without operator intervention, the number of machining steps that required human action have been dramatically reduced.

On some CNC machine controllers, the available memory is too small to contain the machining program (for example machining complex surfaces), so in this case the program is stored in a separate computer and sent direct to the machine. If the computer is connected to a number of machines it can distribute programs direct to different machines as required, one block at a time through a DNC server (Zhekun, 2004).

Adding wireless capability on the shop-floor, it is possible to simplify installation, eliminate cabling, and make machine tools mobile with wireless networking. In addition, there is no need for re-running cable when CNC machines are moved, which is proper to constant shop-floor layout changes, as show in Fig. 3.

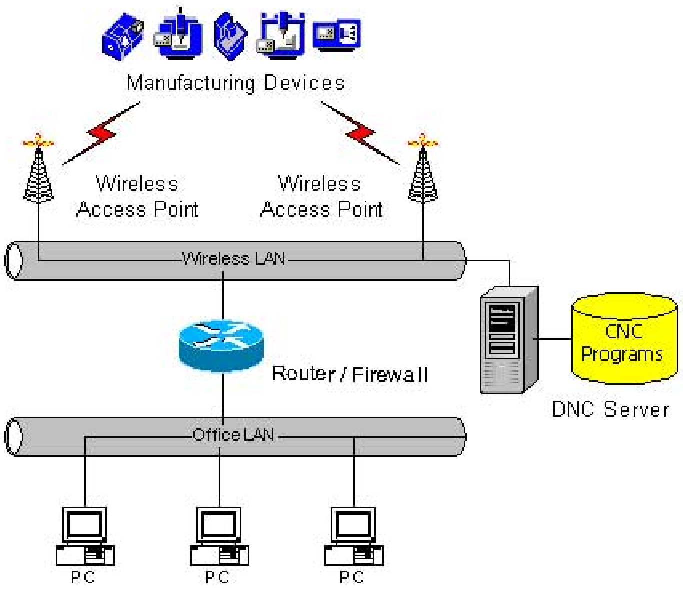

Figure 3. One possible configuration of a wireless network on the shop-floor (Sfa, 2007)

Through wireless ethernet adapters, devices can communicate with a wireless access point placed anywhere on the user's wired DNC server network. Once installed and implemented, the wireless LAN can communicate with all machines placed anywhere within a manufacturing facility. These cable-free machines can be moved at will anywhere within that facility. Changing cable numbers and reconfiguring software or hardware is no longer necessary. The systems available conform to the 802.11 high rate specification, which means it goes beyond machine tool automation to provide mobile network access for laptops, mobile desktops, printers, barcode scanners, PDA devices, and web cams with the use of wireless PC cards. Adding high-gain antennas on its access points makes building-to-building communication possible and allows connection at up to 16 kilometers from the access point (Henning, 2002).

Regarding the network and DNC configuration it depends on the current network infrastructure, security policies, and shop-floor usage. The options vary depending partly on the capabilities of the firewall being used and the IP architecture, but one possible configuration is shown in Fig. 3.

Another solution is to have the DNC server and the CNC programs on the secure office LAN and just the CNC machines on the wireless shop-floor network. And a third option is to use a firewall to completely separate the wireless shop-floor network from the office network. The DNC server is dual homed (two network cards) to allow access to both the wireless shop-floor network and the office LAN.

Unlike other conventional, expensive shop-floor data collection systems, the employees do not have to walk over to a fixed computer workstation and physically type in their information, leaving room for errors, and the loss of valuable production time. In case the current method of data collection is manual, wireless technology allied to automatic shop-floor data collection, eliminates the manual identification sheets, which are frequently damaged, lost, or misplaced (Hum, 2001).

Besides the WLAN's, an alternate is the use of Bluetooth serial ports at the CNC, where the operator does not have to phyiscally connect a wire from the CNC to the notebook, eliminating grounding problems and tripping on the cable.

Using encryption and spread spectrum technology it can be assured security and interference resistance to the wireless network. Thus, the deployment of wireless on the shop floor gives flexibility that saves time and drives down costs while providing secure, mobile access to the networks. This way, it is possible to increase shop efficiency and employee productivity.

4. DEPLOYMENT ON THE SHOP-FLOOR

This paper proposes an analysis of wireless deployment on the shop-floor, based on questions about security aspects, cost and integration of wireless nodes into existing wired network systems, among others, to identify which requirements are needed for each case. For this purpose, it was designed a survey questionnaire considering the mentioned aspects.

4.1 Survey questionnaire

The objective of this questionnaire is to supply a script to wireless deployment on the shop-floor. The questions that compose such questionnaire are divided in five major issues, as described below:

1. **Initial Requirements Survey**
   (a) How many network points will be used in the deployment?
   (b) Which is the service quality desired?
   (c) Which are the devices with interaction priorities?
2. **Physical Characteristics of the Shop-Floor**
   (a) Which is the distance between the extremities of the considered environment?
   (b) Are there considerable physical obstacles among the terminals?
   (c) Are the plant sectors distributed in outdoor or indoor locations?
3. **Current Network System**
   (a) Is required a substitution of the existing network for a wireless network or an integration between both?
   (b) Is the network under constant update and/or maintenance?
   (c) How is the complete description of the current network state?
4. **Information Systems**
   (a) Does the shop-foor possess any monitoring system?
   (b) Are there any CNC machines on the shop-floor? How are they connected?
   (c) Do existing softwares support wireless technologies?
   (d) Was the interface layer (man-machine) implemented separately of the communication layers?
   (e) Do the applications possess access control?
5. **Security**
   (a) Which is the security level desired concerning the choice of data encryption?
   (b) Will the access be restricted?
   (c) Is there any need for internet access?
   (d) Is deployment of RADIUS server required?
   (e) Will the facility work with Virtual Private Network (VPN)?

4.2 Deployment based on the responses

Based on the responses to the questionnaire presented previously, is possible to conclude whether the adoption of the wireless communication is viable or not for the environment in study. It is important to highlight that each environment possesses its particularitities such as: interference and noise levels; physical obstacles; shop-floor extension and specific characteristics of each involved machine. Such particularitities demand a meticulous analysis by the wireless specialist.

According to the initial requirements survey and the physical characteristics of the shop-floor responses, the necessity and the number of access points can be defined. Unless a relatively small number of users is assumed, multiple access points might be required to separate users onto non-overlapping channels to reduce medium access contention and collisions. Reinforcing that the greater the number of wireless clients associated to one access point, the slower the speed will be for each client.

Concerning the physical characteristics of the shop-floor, the most common factors that can determine the speed and coverage of the wireless connection include electromagnetic interference and physical obstacles. Generally, the closer one is to an access point, the faster one's connection will be. While the coverage mainly depends on the output power of the transmitter (wireless card or access point), its location and frequency used to transmit data.

Regarding the current network system, it is important to outline the overall status and configuration of the current network system, identifying whether substituting the existing network or integrating both. The integration can offer lower deployment costs compared with setting up a separate wireless network, besides, for a large enterprise there is often a strong need to access applications and servers on a wired network.

With the information systems responses, it might be necessary to update or replace existing softwares, once they do not support wireless technologies. The implementation of the interface layer separated of the communication layers may facilitate the deployment of new network technologies. And, since there are CNC machines, the deployment of a wireless DNC system must be considered. In addition to it, wireless sensors can collect information and pass to monitoring systems as MES (Manufacturing Execution System), SCADA (Supervisory Control and Data Acquisition) or ERP (Enterprise Resource Planning) in the back-end.

In order to fulfill the security aspects required, a proper type of authentication and encryption must be considered. One simple way is the use of MAC authentication of wireless clients, which means that only traffic from authorized MAC addresses will be allowed through the access point. This can be done determining if a particular MAC address is valid by checking it against either a RADIUS server external to the access point or against a database within the nonvolatile storage of the access point. To reinforce security might be necessary to use a Wired Equivalent Privacy (WEP) encryption protocol and/or Virtual Private Networking (VPN) software, which uses advanced encryption mechanisms designed to be an industrial strength.

Even after conducting a very detailed site survey and deploying a wireless network, ongoing monitoring and fine-tuning must take place in order to ensure optimal performance and security. Changes such as moving the location of antennas or adding more access points might be required besides continued monitoring and maintenance.

5. AN INDUSTRIAL CASE STUDY

In order to check the main issues that affect the implementation and utilization of wireless networks, the questionnaire described on the previous section was applied to an industrial case study. In accordance with the obtained responses, a wireless network was deployed and tested.

The analysis, deployment and tests were placed in a furniture industry which encompasses 13 thousand square meters. On the shop-floor, there were machines with computerized cutting system, painting machines, panel saws, drills for high production amongst others.

5.1 Equipment and machines

The equipment used during the tests consisted of two notebook computers, both equipped with wireless network cards which support data rate up to 54 Mbps. To investigate and get a total network traffic control between the terminals, it was utilized a management and traffic shaping software called Bandwidth Controller 0.31, while the operating system installed on both computers was Windows XP Professional with Service Pack 2.

On the shop-floor, there were basically 32 painting machines with power varying from 160 to 200 kwatt, noise levels at 87,95 dB and average height of 1,5 meters. Besides, 5 drills for high production with power varying from 30 to 50 kwatt, noise levels at 90 dB and average height of 2 meters. Plus, 2 panel saws with power of 35 kwatt, noise levels at 86 dB and height of 1,8 meters. All of them operating with frequency at 60 Hz. Some of these machines can be seen in Fig. 4

Figure 4. Some of the machines found on the shop-floor in study

5.2 Test methodology

As means to analyze all the possible interferences and the security level on the shop-floor, it was performed some consistency and security tests during packet exchanges between two notebook computers in several localities of the plant with distances varying up to 200 meters. The equipment and machines used in the tests were describe in the section 5.1 , plus the physical conditions whose analyses were based on.

The packet exchange process was made through an ad hoc network set up between the two terminals. The choice of the ad hoc mode, contrary to the infrastructure mode, is justified by the fact that the success of its deployment, regarding physical issues as noises and interferences, would make possible the infrastructure mode deployment as well.

Concerning security aspects, these were analyzed through the use of shared authentication network, which enables the use of the same strong authentication credentials by all network members, plus data encryption provided by WEP security protocol. Prior to starting tests, a deliberate access attempt on the pre-configured network was performed. As expected, WEP demanded to enter a password. Then, a monitoring software (ManageEngine WiFi Manager 4.0 Free Edition) was utilized to monitore the network as well as the airspace, in order to detect wireless threats as rogue attacks, intrusions, sniffers, DoS attacks and vulnerabilities.

The tests were performed at least in two different environments. First in the office environment were there were no machine interference, besides some obstacles as doors, office partitions and walls. Then in the shop-floor environment where besides physical obstacles there were electromagnetic interference. For each test set 100 packets of 200 bytes each were sent from one terminal to the other varying the distance between them.

5.3 Results

As mentioned previously, each environment possesses its particularitities such as: interference and noise levels; physical obstacles; shop-floor extension and specific characteristics of each involved machine. Thus, the tests performed in this case study were divide into two different environments which are described subsequently.

5.3.1 Office environment

The tests performed in this environment served to evaluate the network performance without the interference of the machines on the shop-floor. First tests with side-by-side terminals (no obstacles) were performed, later with the presence of glass and wood office partitions as obstacles and finally with wood office partitions and concrete walls as obstacles. The obtained results can be observed in the Tab. 1.

Regarding the interference type: (a) means terminals side-by-side with no interference, (b) means glass and wood office partitions as obstacles and (c) means wood office partitions and concrete walls as obstacles. While network delay means the average number of milliseconds packets spent in transit.

The presented results show that even with the presence of the described obstacles, neither the communication nor the quality of signal between the terminals were significantly affected.

Table 1. Packet exchange in the office environment

Test	Interference Type	Network Delay (ms)	Packet Loss	Distance (m)	Connection (Mbps) Terminal 1	Connection (Mbps) Terminal 2
1	a	1,1	0	0	54	54
2	b	1,1	0	5	54	54
3	c	2,9	0	5	54	54
4	c	3,0	0	10	54	54

5.3.2 Shop-floor environment

The tests performed in this environment were submitted to noises from 87 dB to 92 dB with distances between the terminals varying from 0 meter (side by side) up to 200 meters. Beyond the proper machines present on the shop-floor, whose maximum height reached 2 meters, there were not further obstacles between both terminals. The obtained results can be observed in the Tab. 2.

Table 2. Packet exchange in the shop-floor environment

Test	Interference Type	Network Delay (ms)	Packet Loss	Distance (m)	Connection (Mbps) Terminal 1	Connection (Mbps) Terminal 2
1	d	1,1	0	0	54	54
2	d	2,2	0	10	54	54
3	d	3,1	0	20	48	36
4	d	3,8	0	35	24	36
5	e	4,5	0	50	24	36
6	e	7,6	0	70	5,5	11
7	e	9,8	0	100	1	1
8	e	10,5	0	150	1	1
9	e	12,5	0	200	1	1

Regarding the interference type: (d) means terminals side-by-side (no obstacles) but with machine interference and (e) means machines as obstacles and interference. While network delay means the average number of milliseconds packets spent in transit.

The presented results show that as the distance increases the quality signal between the terminals diminishes. Even though, the packet exchange was performed successfully up to 200 meters despite the distance and machine interference on the shop-floor.

5.3.3 Discussion

The tests performed both in the office environment and in the shop-floor environment showed satisfactory results, in terms of security, quality of signal, packet exchange, connectivity, noises, data integrity and external interferences. The choice of ad-hoc mode instead of other possible communication for standard 802.11 and WEP protocol amongst the existing ones was purposed, because once such choices succeeded other configuration types would suceed as well. The packet exchange even in distances of up to 200 meters proved the low interference, caused by machines on the shop-floor. The noticed security, was mere representative once the set up network was small and of few participant devices. The WEP protocol, even weak and vulnerable, was safe enough for the situations in study. However, an increase in the security issue could be possible with protocols more consistent as the WPA (Wi-Fi Protected Access) or the adoption of a specific network monitoring software. The quality of signal, notably low in certain situations could be increased with the addition of one or more access points, altering the network from ad hoc to infrastructure formation. The addition of access points would increase the network coverage area besides the participant device number.

6. CONCLUSIONS

The data communication networks play an important role in the integration of a flexible manufacturing system, either in the individual equipment level, which needs interfaces and communication protocols; the cell level, through the cell management (control system network connected); as the overall system level, integrating all the system components (purchases, marketing, engineering, warehouse, etc.).

As presented in this paper, the wireless technology is poised to advance shop management's ability to control and monitor shop events as they occur besides adding a significant degree of independence in a shop's operation. Once, it is possible to simplify installation, eliminate cabling, and make machine tools mobile with wireless networking. This lack of need for re-running cable when CNC machines are moved, it is proper to constant shop-floor layout changes besides workers can access part and process specifications from locations where wired networks are impractical.

The analysis described along this paper, which is based on questions about security aspects, cost and integration of wireless nodes into existing wired network systems, among others, serves a script to wireless deployment on the shop-floor. From the responses obtained through the questionnaire presented it is possible to conclude if the adoption of the wireless communication is viable or not for the environment in study.

The tests performed in a case study, showed satisfactory results, in terms of security, quality of signal, packet exchange, connectivity, noises, data integrity and external interferences even in distances of up to 200 meters in a ah hoc formation, which reinforces the wireless network reliability.

This way, despite some companies may have reservations about implementing a wireless network on the shop floor, it is quite possible to operate with up-to-date information concerning collection and synchronization of real-time shop-floor data in a automatic or semi-automatic approach, which improves the data reliability, reduces the cost and increases shop efficiency and employee productivity.

7. REFERENCES

Brewer, A., Sloan, N., Landers, T., 1999, “Intelligent Tracking in Manufacturing”, Journal of Intelligent Manufacturing, Vol. 10, No 3-4, pp. 245-250.

Crow, B.P., Widjaja, I., Kim, L.G., Sakai, P.T., 1997, “IEEE 802.11 Wireless Local Area Networks”, IEEE Communications Magazine, Vol. 35, Issue 9, pp. 116-126.

Henning, R., Henning, B., 2002, “Wireless Job Shop Data Collection: Issues and options for Job Shops Solutions”, PMPA Technology Software Conference.

Huang, G. Q., Zhang, Y. F., 2007, “RFID-based Wireless Manufacturing for Real-Time Management of Job Shop Wip Inventories”, International Journal of Advanced Manufacturing Technology, (Accepted for publication).

Hum, A. P. J., 2001, “Fabric Area Network - A New Wireless Communications Infrastructure to Enable Ubiquitous Networking and Sensing on Intelligent Clothing”, The International Journal of Computer and Telecommunications Networking, Elsevier, Vol. 35, No 4, pp. 391-399.

SFA Shop Floor Automations, 4 April 2007, <http://www.shopfloorautomations.com/wirelessdnc.php>.

Tse, D., Viswanath, P., 2005, “Fundamentals of Wireless Communication”, Cambridge University Press.

Zhekun, L., Gadh, R., Prabhu, B. S., 2004, “Applications of RFID Technology and Smart Parts in Manufacturing”, Proceedings of DETCŠ04: ASME 2004 Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Salt Lake City, Utah USA.

8. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.