

## Feature Article

### Modern Machine Shop-May 2006

#### No Wires, No Worries

Is it safe to make your shop floor a “hot spot” for wireless DNC and other data communication? This shop’s experience shows that it is.

By [Mark Albert](#)

Sometimes it takes a bolt of lightning for a company to implement a new technology. That’s literally what happened at Miller Welding and Machine in Brookville, Pennsylvania. When lightning struck the company’s main plant in October 2004, the current followed the network cables connecting most of its machining centers. The surge of energy destroyed critical circuit boards inside the CNC units, taking the machines out of commission and seriously disrupting production. It took several days and thousands of dollars to get this equipment back online.



Machine tools at Miller Welding and Machine Co. operate near arc welding stations and under electrically powered cranes. Wireless DNC works well in this environment.

According to Mike Carrier, Miller’s engineering manager, that experience convinced the company to install a wireless network for downloading data such as NC programs to machines on the shop floor (a procedure often called DNC for direct or distributed numerical control). This wireless network replaces the cables that physically connect the machine tool CNCs. “Fortunately, we had only three machines active at the time, or we might have lost more from the lightning strike,” Mr. Carrier says. The shop had been planning to connect all of its CNC machines to this network, but the expense and difficulty of stringing wire across the factory to reach additional machines had delayed further progress.

A network that does not need wired connections obviously avoids that obstacle and would make it possible for Miller to use DNC on all of its CNC machines. Wireless connections (often called WiFi for “wireless fidelity” in computer circles) also promise to make it simpler, easier and less costly to move this equipment. That was an important consideration because Miller is a growing, changing company that increasingly relies on its ability to respond to its customers’ needs by adding or relocating production assets.

However, the company had some reservations about implementing a wireless network on the shop floor. Could a WiFi network reliably transmit NC programs with no errors or corrupted data? Would it be fast enough to keep up with a machine’s demand for toolpath data? Could NC programs be intercepted by eavesdroppers trying to capture confidential information about a customer’s product designs? Could a hacker get into the company’s databases by tapping into the wireless system? In addition to these concerns, which many shops share, Miller had one more question. The shop had two systems in place for downloading NC programs, and the second system included a dedicated library of programs created on conversational controls. Could one wireless network be used with both systems without making this library of programs obsolete?



As Eric Miller looks on, Mike Carrier scrolls through a list of machine tools connected to the shop’s wireless DNC system. With eXtreme DNC software, he can monitor the downloading of NC programs anywhere in the plant from his desktop PC.

With assurances from the WiFi system provider, the company installed a wireless network in May 2005. Since then, all of the former concerns have proven groundless. Dozens of NC programs are being transmitted wirelessly every day, and at press time, there has not been one case in which the system failed to download an NC program successfully. Every download has been free of transmission errors—which is a better record than that achieved by the hard-wired network. Scrambling the data at the point of transmission and unscrambling it when it is received prevents outsiders from intercepting usable data, and a “virtual private network” makes it impossible to access the shop’s databases through the DNC system. Of special interest to Mr. Carrier is the fact that the wireless system functions equally well with both of the shop’s existing systems for sharing NC programs.

This success is all the more remarkable because the shopfloor environment in this plant appears to be a hostile one for a WiFi network. The company is named Miller Welding and Machine for a good reason: It does a lot of electric arc welding.

Manual and robotic arc welding stations are located throughout the plant. Many are located next to the shop's large vertical and horizontal machining centers and CNC lathes. Plasma cutting tables are also near some of the machine tools. Most of the machining bays are served by large, electrically operated overhead cranes with open sliding contacts. These numerous sources of radiant electrical energy are notorious for creating "noise" and interference that can disrupt radio signals or affect the data that they carry.

John Carpenter, president of [CNC Computer Integration](#) (Ellington, Connecticut), the firm that supplied the wireless network, describes Miller as "one of the toughest environments you can imagine for a wireless network." The fact that such a network performs flawlessly there, he says, makes it "a great example of how reliable and trustworthy WiFi can be on the shop floor."

One of the main advantages of wireless technology has already benefited the shop. Mr. Carrier explains: "Since putting in the wireless network, we've moved several of our machining centers to make room for new machines. With no cables to move or reroute, we just picked up the machines and moved them to their new locations. The wireless connection moves with the machine."

### On The Move

That Miller needs to move machines around to make room for new equipment reflects the growth and development that the company is experiencing right now. Founded by David R. Miller in 1963 as a repair shop, the company's main plant has been located next to Sandy Lick Creek, about a mile from Brookville's historic Main Street district, since 1971. This facility has undergone numerous expansions as the company became an integrated, single-source contract manufacturer. Mr. Miller's expert welding skills and machining know-how guided the company during its early years, until his sons, David K., Bradley and Jeffrey, could help with day-to-day management of the company. The elder Mr. Miller, who serves as chairman of the board, continues to work in the shop and monitor its progress. His wife, Sara, runs the front office. A grandson, Eric, who has a degree in computer science, heads up the IT department.

Today, the company has around 300 employees. Its Sandy Lick site has 93,000 square feet of manufacturing space. In 2000, the company purchased a new site on the other side of town not far from Interstate 80 and constructed a 120,000-square-foot facility there for complete fabrication services. Known as the Maplevale plant, it houses large dedicated welding stations (most of them automated with robots), a laser cutting machine and two complete paint finishing lines. One of these is automated and is capable of handling parts as long as 12 feet and weighing as much as 5,000 pounds. The second line allows even larger and heavier workpieces to be powder- or wet-coated.

The capacity of these coating lines is a good indication of the large workpieces for which Miller is best known. One of its specialties is welded fabrications for the mechanized construction industry. The company has contracts with some of the best-known builders of construction and off-road vehicles in the country.

Because large workpieces are prevalent, the company has about a dozen large vertical and horizontal CNC machining centers. Almost all are four-axis machines with 50-taper spindles in the 20- to 50-horsepower range. Milling and drilling are the main operations performed on these machines. Several lathes are used for jobs such as turning large rolls that have been repaired or restored with welding. Steel is the most common material, but the shop also machines a substantial amount of cast iron. The company can cut steel plate as thick as 12 inches for weldments; many of these pieces are machined at the main plant.

Currently, all of the company's CNC machining centers and lathes are at this location. Only the machines slated for replacement have been left off the wireless network. Several CNC plasma arc cutters are also networked wirelessly. Although no CNC machines at the Maplevale facility are connected yet, the framework for a wireless network is in place there, too.

## Wireless Networking Basics

Before the fateful lightning strike, Miller was running eXtremeDNC software from [Ascendant Technologies](#) (Aliso Viejo, California). This software had been installed by MACDAC Engineering, Inc. (Somers, Connecticut) in 1998. When wireless communication first started to be deployed on the shop floor, the communications division of this company split off to form CNC Computer Integration. This new company's main focus is on providing wire-free solutions to manufacturers, so it was natural for Miller to choose CNC Computer Integration for the new wireless network.



The wireless access point and antenna are mounted to the ceiling above a machining area. The access point is wired to the DNC server and is powered without a separate electrical line.

According to Mr. Carpenter, a wireless network consists of one or more data access points (the radio units that are connected to a shop's data communications center) and a wireless interface that is physically connected to the machine tool. In a wireless environment, NC program files are downloaded from a central file server in a procedure that is basically the same as on a wired network. Although there are some important technical issues associated with wireless technology, they are largely transparent to the end user, a fact that Mr. Carrier was relieved to find out. "I didn't want to become an expert in WiFi systems in order to get our wireless DNC network up and running in the plant," he says.

For most industrial applications, access points are mounted to the ceiling overlooking the equipment to be networked. For data transmissions, WiFi networks must operate on a band of radio channels set aside for these applications, as governed by Federal Communications Commission (FCC) specification 802.11b. These channels have a frequency of 2.4 GHz. According to Mr. Carpenter, this high-end frequency is suitable for shopfloor broadcasts because signals of this wavelength literally bounce off machinery and readily create echoes, thus enhancing reception within the broadcast range.

Today's WiFi technology allows data to be transmitted at high speeds—as high as 11 million bits per second. Even at the lowest settings for transmission speed (1 million bits per second), there is plenty of bandwidth for as many as 100 machine tools to download programs simultaneously from a single access point. As Mr. Carpenter points out, most CNC machine tools already in place have data communication speed that is restricted to the limitations of RS232 serial ports, which is typically 96 baud (9,600 bits per second). Even on the latest CNCs with high speed Ethernet-based data communication (roughly ten to 100 times faster than RS232), downloading is well supported by current WiFi capabilities.

What is important to understand, Mr. Carpenter stresses, is that not all commercially available wireless access points are of equal quality or capability. "The right technology is necessary for error-free, secure data communication," he stresses. "This technology has to allow transmitted signals to be distinguished from stray radio waves—noise and interference—and do so flawlessly." His company has chosen RoamAbout Wireless Access Points from Enterasys (Andover, Massachusetts) because he believes these devices provide the best basis for secure and reliable data transmissions.

As Mr. Carpenter explains, the technology behind these access points is based on the characteristic square waveform of the data signals it exchanges. "Noise," by contrast, typically follows a sinusoidal (rounded) waveform. Bursts of electrical energy, such as those emitted when a welder strikes a spark, follow such a crest-and-valley pattern. The difference in waveforms allows high-quality wireless devices to distinguish and accept only the square data signals and ignore the rest. That, in simple terms, is what makes two-way wireless communication practical in industrial settings.

Likewise, the wireless interface at the machine tool makes a special application such as DNC both practical and affordable. CNC Computer Integration has developed a wireless DNC interface device called WireFreeCNC. It uses the same wireless communications technology commonly used for wireless laptop computer connections to exchange signals with the access point. The wireless DNC device accepts a plug-in PCMCIA wireless network card. This card "talks" to the access point at the 802.11 frequencies designated for WiFi applications. The DNC device, in turn, "talks" to the CNC. It does this by converting WiFi signals into the serial-stream format required by the standard RS-232 communications port. (The WireFreeCNC device is available for Ethernet connections as well.)

"We went with an off-the-shelf plug-in wireless radio network card because that approach makes it possible for us to adopt new communications technology as it becomes available without having to change the DNC device with each upgrade," Mr. Carpenter says. He adds that the access point and network card have other important

functions. One is running an error-checking protocol during data transmissions. This software routine automatically checks the completeness and accuracy of data transmissions by checking certain numerical values attached to each packet of data. If these values do not add up to the correct sum each time, then the software detects that each data packet sent has not been matched by a data packet received. A request to resend the missing packet ensures that no data are left out when the transmission is complete.

Another important function of the access point and network card is to handle certain data security procedures.

## Data Security

Making sure that data gets to the machine tool without errors is certainly a requirement of a wireless DNC system. Ensuring that data doesn't get into the wrong hands is an equally important requirement.

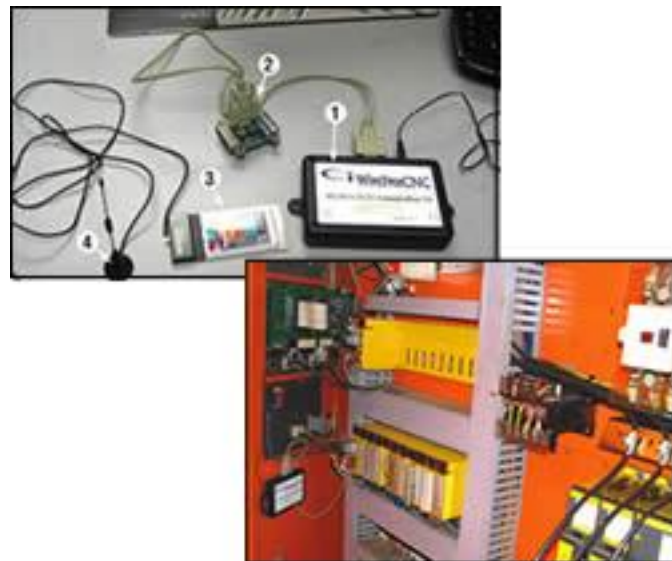
According to Mr. Carpenter, securing data on a wireless network has to take a multi-pronged approach. For one thing, data security must address two concerns: 1) how to prevent usable data from being intercepted by unauthorized parties, and 2) how to prevent access to a corporate network through wireless links. He says that shops have a tendency to worry too much about the first concern while being less mindful of the second.

Wireless networks can take several steps to thwart eavesdroppers. According to Mr. Carpenter, each step represents a higher level of privacy protection. The most basic procedure is to implement some form of encryption. This simply means encoding messages before they are transmitted and then decoding them when they are received. One form of encryption, 128-bit WEP (Wireless Equivalency Protocol), can be applied by the access point and the wireless network cards. Essentially, this form of encryption attaches a string of digital characters to each packet of data. Unless the receiving device has the digital key to unlock this string of characters, the data packet cannot be read. This form of encryption is in force at Miller. It appeals to Mr. Carrier because, as he puts it, "only the data in the air is encrypted."

Also available is Wireless Privacy Authentication (WPA), by which communicating devices must exchange a user name and password to initiate messaging. This is also a protocol that is observed at the access point and network card level. Another approach, called MAC filtering, takes advantage of the ID number (Media Access Control) assigned to every communications device by the manufacturer. Communicating devices can be set up so that only the devices whose MAC identifiers are listed as approved recipients will be permitted to exchange messages. Any device not on the list will be filtered out as ineligible.

Mr. Carpenter stresses that network security and data privacy techniques are always evolving. By keeping these measures in the components that are most easily replaced or upgraded, such as in the plug-in radio network card, a wireless shop network has the best chance of keeping up with these advances on a practical basis.

Keeping hackers out is also readily achievable. "The key concept here," Mr. Carpenter says, "is to isolate the wireless network from the corporate network, with a bridge between the two controlled by the company's IT department." That way, if unauthorized parties gain access to the wireless network, they cannot cross over to the corporate network and its databases. The approach taken by Miller is to use a form of "multi-honing" on the



This is what goes into the machine tool's electrical cabinet: 1) a communications interface device; 2) a "wedge" pin socket connector for the RS232 port; 3) a radio network card, which plugs into the interface device; and 4) a whip antenna for mounting on an exterior surface of the cabinet. The picture to the right shows these components installed in one of Miller's machining centers.

corporate network. Multi-homing simply means creating more than one network connection for moving data from the file server to the network.

In this case, Eric Miller added a second network communications card at the DNC file server in his IT department. This card is dedicated to the wireless shopfloor network. Messages exchanged through the second network card use “non-routable” addresses—that is, destination codes that can be reached only on that part of the network. In a word, wireless traffic cannot pass to routes not governed by the dedicated network card. There is no way for an intruder to enter the corporate network from a wireless connection because the grids are separate and only bridgeable by the IT department.

### **Simple To Install**

Mr. Carrier reports that building the wireless network was not difficult. It involved four steps: 1) planning for the system, 2) installing the access points and file server, 3) installing the CNC interface devices and 4) testing the system.

To plan for the system, Mr. Carpenter did a site audit—walking through the plant to determine how many access points would be needed and where they should be located. Because Miller’s Sandy Lick plant has a number of separate bays, he selected four locations (a fifth will be added in part of the plant that’s being converted into a new machining area). Because the bays have high ceilings (15 to 35 feet), finding a central spot roughly in the middle of the machines below was not a problem. The access points have an omnidirectional antenna for exchanging signals generally within a 300-foot radius.

Mr. Carrier arranged to have the access points mounted by the company’s maintenance staff. Access points are hard-wired to the file server but are powered through the network cable itself, so no separate power line is required. An access point was also installed at the Maplevale facility at this time.

Installing the wireless DNC devices at each machine tool was equally straightforward. CNC Computer Integration provided a kit for each machine. The typical kit includes the WireFreeCNC interface box, a plug-in PCMCIA radio card, an RS232 Inline Wedge and a whip antenna on a magnetic base. The interface box is mounted inside the electrical cabinet of the machine tool. The Inline Wedge connects the interface box to the RS232 port but adds a second pin connector socket so that it can “wedge” this new device between any external devices that may already be interfaced to the communications port without disrupting them. Most ports have one pin for a low-voltage power supply, and this is sufficient to operate the interface box. Otherwise, a 9- to 36-volt AC or DC transformer can be plugged into a 110-volt outlet to power the device. The whip antenna, wired to the interface, is placed on the outside of the electrical cabinet. Mr. Carrier estimated the installation for each machine at about 1 hour.

To test the system, he and Eric Miller went to each machine with a laptop computer and logged onto the DNC system from the laptop through the wireless connection. First, they made sure that the network address assigned to the CNC matched one of the addresses served by the appropriate access point so that the CNC knows which access point to talk to, so to speak. Then they initiated a program download and checked to see that the program was received successfully at the CNC.

The 11 Mazak machining centers received slightly different treatment. These machines all have Mazatrol CNCs for shopfloor programming, but the programs are archived on a dedicated workstation running Camlink software from [Griffo Brothers, Inc.](#) (Corvallis, Oregon). This workstation was linked to the machines via a multi-port switchbox, creating a mini-DNC system of its own. Now, the workstation is connected by wire to the DNC file server, but wireless connections in the CNCs make using the switchbox unnecessary. Programs selected at the workstation are uploaded to the DNC server for wireless downloading to the machines. “Our library of programs in the Mazatrol format is more secure and downloading is now less complicated since removing the switch box.” Mr. Carrier says.

### **More Than Cable Replacement**

Although WiFi has proven to be an effective way to download NC programs, creating a wireless hot spot on the shop floor opens up other possibilities that excite Mr. Carrier. A wireless infrastructure supports numerous applications in which the ability to transmit data immediately and with mobility has value.

Miller already has a good example in place. It uses a portable FaroArm coordinate measuring machine from [Faro Technologies, Inc.](#) (Lake Mary, Florida) to inspect many of the large workpieces it produces. The flexibility, accuracy and reach of this arm make it ideal for such purposes. Using the wireless network to transmit measurement data makes this device easier and quicker to move and set up. Likewise, corrective feedback to manufacturing processes can be delivered instantly via a wireless connection.

Mr. Carrier is also looking at the point-of-use “candy-machine” tool dispensing units that are located in several locations across the shop. A wireless connection at these units would streamline restocking routines, thus saving many footsteps, and make re-ordering procedures more precise and timely.

Ultimately, however, these projects are overshadowed by what Mr. Carrier sees as a more revolutionary vision for manufacturing that is contingent upon a wireless environment. In this vision, all material movement and process activity would be monitored by radio signals from anywhere on the shop floor. In a passive mode, developments such as RFID (radio frequency identification) would track the location and status of work in process and monitor critical process elements such as cutting tools, gages and fixtures. In an active mode, personnel with handheld devices could signal the start and finish of operations, send work activity reports, count inventory and receive assignments or instructions, all in real time.

Mr. Carpenter shares this larger vision for the role of wireless technology on the shop floor. In fact, this vision represents the direction in which his company is moving in wireless product offerings and development. The company now offers a number of products under the WireFreeShop brand. These include a wireless terminal for entering shop control data, time and attendance, bar code reading and so on. Remote trouble diagnostics is also under development. Several customers are well on their way to implementing these concepts.

“Eliminating cables to machine tools makes a lot of sense,” Mr. Carpenter says, “but it represents only a small part of the value that WiFi creates on the shop floor.” As he sees it, uncabing CNC equipment isn’t nearly as important as unleashing the imagination.