6 Critical Things to Know Before Implementing Wireless on the Plant Floor

This articled was prepared by Siemens Industry and appeared on Automation Worlds website October 5th, 2009

While the automation command "startup" may not be as historically significant as the dots and dashes of the Morse code "SOS" distress call, it is no less important to the day to day operation of the factory machine that won't go unless it gets the instruction to begin operation.

According to industry analysts, those instructions are being transmitted more often via wireless networks than ever before. In 2007, industrial customers bought some 2.7 million wireless enabled factory automation devices – predominantly rugged mobile computers, sensors and remote I/O – a number that is projected to almost triple to 8 million by 2013, reported Wellingborough, UK-based IMS Research in March 2009.

Much of this growth is driven by the reduced costs and faster start up times promised by wireless technology. If you don't need cables then you don't have to pay for them or install them, but it's not all as simple as it sounds. Wireless adoption has had its hurdles: the most significant of which are reliability and conservatism among the target market.

The presence of heavy machinery or a shielded wall won't often disrupt the signals travelling by cable, but they can significantly disrupt a wireless signal if the transmitters and antennae haven't been positioned correctly. When combined with a rise in the value placed on dependable, detailed machine data and an "if it ain't broke" attitude these factors have combined to inhibit adoption.

Obviously, as IMS' projected market growth indicates, these inhibitors are being rapidly overcome, as the relative cost of wireless enabled devices falls, more ruggedized wireless products hit the market and global economic conditions make the potential cost savings more important than ever before, prompting companies to experiment and launch pilot projects.

"Not many people are going all in yet," says Marty Jansons, a spokesperson for Siemens Industry, Inc. "However we are seeing more and more demand for wireless systems on the shop floor in a variety of industries. Along with that we are getting a lot more people asking us what they should be thinking about when they start looking at wireless."

"There are two camps when it comes to wireless: people are either scared of it or they aren't and it's the second group that make me nervous," says Todd Preder, a business development manager with Professional Control Corporation, a Wisconsin-based automation distributor which helps customers set up industrial wireless networks. "The people who are more cautious generally have more success. It's not something that should be taken lightly."

In keeping with that Jansons has put together a list of six things that customers should consider when they start thinking about rolling out a wireless solution.

1. Have a clear idea of what you want to accomplish in both the short term and long term with the wireless network.

Planning ahead is key, stresses Jansons, adding that laying the groundwork for future applications will save time and money in the long run. “We’ve often seen wireless used for monitoring, warehousing, diagnostics and I/O control applications essentially as a cable replacement system,” he says. “But that’s only a fraction of the potential applications. We’re already seeing it being deployed to enable seamless roaming between indoor and outdoor for wireless VoIP communications, RFID, Automation monitoring, wireless work tablets, PDA’s and I/P based video surveillance.”

2. Be familiar with wireless standards. Understand the particulars of each standard and how they support wireless applications.

There is a wide variety of offerings available in the market -- Bluetooth, Zigbee, multiple flavors of 802.11, and proprietary 900 Mhz, standards. And they are in a constant state of flux. For example, at the beginning of September the ISA 100.11a industrial automation standard was passed. Each has its own strengths and limitations. Are you a discrete operation, or continuous process? If the former you should stick with 802.11, whereas the ISA 100 standard was written with process industries in mind. Which is right for you?

“Different technologies are available that are better suited to different tasks,” says Preder. “For example, most office environments rely on 802.11B or -G so we are trying to get our customers to go with 802.11A so they don’t conflict.”

3. Have a good idea of how reliable the network needs to be.

Some people believe that a wireless application needs to be as reliable as its wired equivalent, but the vote isn’t unanimous which is why it’s so important to know what your particular requirements are. ARC Advisory Group research director Harry Forbes says it depends on the application. “You can add reliability to the network later if you need it. For a lot of applications pretty good is plenty good enough.” This would be true in process type applications, but for most plant-floor applications this would not be the case.

Preder agrees, but postulates that most plant floor apps are unable to compromise reliability. “In our world most applications are going to be I/O and for those you need to be able to depend on it the same way you’d rely on a wired network. From an I/O perspective you are talking about millisecond updates, as opposed to the office environment where you send something to the printer and usually don’t care if it takes a few minutes to get there.”

4. It’s critical that every wireless solution have data security and industry standard encryption methods.

“The security word comes up again and again as an objection to deploying a wireless solution,” says Jansons, but there’s no need for security by obscurity. Security methodologies are there for wireless. It’s just a matter of how deep you want to go.”

Jansons suggests a short list of industry standard wireless encryption methods for anyone building an 802.11 network. “WEP (Wired Equivalency Protocol), WPA (Wi-Fi Protected Access) and WPA2, all provide at the least a base level of protection. Each encryption level incorporates a higher degree of security thus making is more difficult for someone to eavesdrop on a data communication conversation.

5. Understand exactly what capabilities you need from your wireless network.

"Deterministic communications, rapid roaming and environmental ruggedization may all be factors for consideration when rolling out a wireless network," says Jansons. "Or they may not. You need to know what you need before you can deploy it and achieve complete success from your installation."

Forbes agrees. "All of these attributes are dependent on the application. None of these are always going to be required. Roaming is important in in-plant set-ups, ruggedization is only required in harsh environments while determinism is big in automotive and machine control but not in apps that use TCP/IP. A lot of MES apps don't need it, but are greatly enhanced by wireless.

Another application where wireless can enhance communications is in the area of safety. Wireless is already being implemented in control applications dealing with safety, but, due to this being a sensitive area, it is important to fully understand the attributes needed.

"A lot of people are sceptical about I/O wireless, then when you mention safety they really start to freak out. However, it is being done successfully so it is something you may want to be ready for – at least from a future growth perspective," says Preder.

"Most machines with moving parts are outfitted with light curtains or laser scanners to protect personnel working on or near the machine and to provide better positioning accuracy," adds Jansons. "Using 802.11 wireless in combination with safety protocols and failsafe PLCs can reduce cabling costs, maintenance times and shorten downtimes."

6. Perform some kind of wireless site assessment before making an investment.

"You want to understand your surroundings," says Jansons. "You may have blind spots or other areas where interference is going to impact the network or influence the kind of technology you select. Conducting a site survey is important as many of these issues can be resolved before installation."

Jansons recommends enlisting the help of a licensed professional for this, and suggests that end users can call on a number of entities for assistance, including systems integrators, engineering/consulting firms or their automation vendor. However, Forbes adds that the end user can do it themselves. "If you're providing coverage for an area yourself then it's a good idea, but for the sensing apps it's more ad hoc testing than professional. To do feasibility testing, most people just get a test kit from their supplier."

Steve Dickerson, chairman and CEO of CAMotion Inc., an Atlanta, GA-based provider of specialized robotic palletizers and depalletizers to the printing and food and beverage industries, is a huge proponent of wireless technology.

For Dickerson the to-wireless-or-not-to-wireless question comes down to two factors. "You have to ask 'what does it cost to put in wires as opposed to wireless. Then you have to ask about reliability. Stationary systems will be different, but in robotic applications things are moving around all the time so the wires are moving around all the time too. That movement degrades the reliability of the wires and the connectors. In fact, these wires become the primary source of unreliability in the whole system. On the other side, you have to be concerned with interference. We've never had a problem with this, but you have to ask the question and do a survey."