



InTech.

September 20, 2006

Up in the Air

Wireless technology sees more uses, but still faces challenges in some environments

By Ellen Fussell Policastro

Proponents of wireless say it is boosting productivity and making processes more efficient. Skeptics say reliability and security are still bugs wireless manufacturers need to work out. Nonetheless, manufacturers are hooking up with wireless. Aerospace companies use wireless for the manufacture of aircraft where “everything’s bar-coded,” said Richard Rushing, the CSO of AirDefense, a wireless internet engineering task force (IETF) infrastructure protection provider in Atlanta. “They can run real-time wireless functionality directly into their environment. Anything you can barcode or scan or do inventory control of functions well with wireless.”

Nuclear power plants typically use wireless as a communication medium to get a signal from one point to another, or for data shipped back to a central facility, he said. “They have sensing devices out in the middle of nowhere, and there’s nowhere to get data back. “It’s cost prohibitive and physically prohibitive to do that via regular networking technology. When using wireless in a manufacturing environment, it’s typically a mission critical network,” Rushing said.

Rushing referred to one aircraft parts manufacturer that sees wireless as a necessity and cost savings for their work stations, which are mobile pods. “Their whole manufacturing is done solely on wireless, not only on their testing equipment but production,” he said.

Talking turkey

At Carolina Turkeys in Mt. Olive, N.C., the plant deployed a complete wireless communication system for voice, text message, and personal alarm so they could make and receive voice calls and join auto-initiated group conference calls, sending, receiving, and confirming receipt of user-based text messages.

“The main purpose was to help achieve the company’s productivity and safety goals, integrating communications with their telephone system (PBX), process monitoring and control system, and quality control system as well as their production planning and scheduling, networking monitoring and control, security, and building management

systems,” said Tom McKearney, vice president of marketing and business development at Ascom Inc., manufacturer of wireless products in Morrisville, N.C.

The Carolina Turkeys plant is 750,000 square feet under one roof and sits on nearly 1,500 acres of land, with a staff of about 2,500 associates working in multiple shifts. The plant’s massive cooking area was the initial target for wireless integration. The company integrated the wireless platform in the further processing and ready-to-eat areas of the plant in the first phases. To support disaster recovery and instant emergency or group communications, the company also had a mobility server and emergency notification system installed.

It is also important for a wireless system to help manufacturers comply with USDA hazards analysis and critical control point regulations. Carolina Turkey uses wireless to text message to key production staff handsets to avoid product-damaging temperature deviations. Process operator Felicia Boney said “being able to reach a manager, supervisor, or maintenance person without leaving the floor has been an advantage. If I’m busy in the Triple C, and I have a problem in post pasteurization, the phone alerts me immediately,” she said. Key staff in safety, production, and management can also receive alarms directly to their assigned handsets, regardless of where they are in the plant. “Being able to respond more quickly to certain situations can reduce the risk of accidents or even the need for a plant-wide evacuation,” McKearney said.

Challenges still exist

Although some companies are gobbling up the benefits of wireless, it still isn’t without challenges. A worldwide study by IMS Research concluded the number of wireless industrial products working in the field to industrial standards is still low. A lot of wireless hardware that sees use in industry was designed for an office or home environment. But more commercial and domestic grade product installed in industry is seeing use in trial applications—on an experimental basis. Users are cautious about using wireless communications for anything but monitoring, data collection, and program tweaks, the IMS study said. They are concerned about reliability and security, with interference the driving factor, which could be a safety risk.

Speed is one of the biggest issues in wireless, Rushing said. “We’ve finally discovered it’s uncontrollable. Since it’s in the airwaves and you can’t see it, there’s no way to control it leaking out of the building,” he said. “It’s up in the air.”

The second issue is it is pervasive inside organizations. “Any new laptop you buy today has wireless built into it,” Rushing said. “So even if you’ve decided not to deploy wireless, you have issues. You can’t even buy a laptop if you don’t want wireless. Some organizations are “scratching their heads” because they can’t avoid wireless; they have to address it.

The third big thing is it “keeps getting broken,” he said. “New attacks are always coming out with new vulnerabilities just because it’s the new playground for hackers. This

environment makes it easy. Some categorize it as low-hanging fruit in organizations. Would I rather break through your firewall or just drive up to your parking lot pull out my laptop and attack you that way? So a lot of people are doing research on it. It relies on and performs well for new vulnerabilities.”

The fourth issue is, since wireless makes network connectivity so easy, people are using these zero-day vulnerabilities to attack desktop environments. “It’s very hard to protect a client with a wireless card,” Rushing said.

If your wireless network is down, you no longer ship or manufacture goods, and that is a danger, he said. Also the network is sometimes interconnected with the business network, without much protection between the networks. This is where an attacker is likely to strike. Without monitoring of the airwaves, you cannot see what is happening on the network—like doing trouble shooting and performance management in the dark.

Protecting the airwaves

Rushing said one of the things wireless companies in the corporate environment can do to protect their wireless data is use an enterprise software package to watch what’s going on. “Watching the airwaves, such a package can tell you if anything bad is going on to give you some sense of reliability,” he said. Agents built into a client report back to a server to monitor what’s going on when users are not in the office environment or at a convention center for instance.

Designed as a monitoring system to monitor airwaves for wireless attacks and performance anomalies, such a software package can see anything that is wireless in nature, “from someone who’s changed their address on their card to bypass security methods, to someone who’s trying to actively attack a Web key (an encryption key used for a lot of distribution centers that use handheld devices).

If you’re not looking at the airwaves, you can’t tell if someone’s trying to invade. That is because “the medium is converted,” Rushing said. “An access point is plugged into the regular network via Ethernet. It’s a bridge, so it takes information into the wireless mode and puts it on the Ethernet and takes information from Ethernet and sends it to the wireless side. It’s kind of like it’s being translated from one to the other. If you’ve missed things when it’s being translated, wireless has its own control and management frames that don’t necessarily get converted from one side to the other. So if something’s going wrong, you can’t figure it out just by looking at Ethernet.”

Where standards stand

Real growth in wireless demand is what will encourage large companies to develop industrial grade products, said the IMS study. But time will tell; manufacturers are still digesting customers’ requirements for Ethernet products. Users will probably become more confident as standards become a stable platform for automation systems, the study said. Technological developments and user knowledge will help prod the process.

Currently, 802.11 has standards from transmission, and other things, that were left out of the original standard, Rushing said. “The standards keep changing to take care of management, deployment, performance, and security issues, and will continue to change in the near future.”

The big security standard was supposed to be 802.11i, Rushing said. “But it left out management and control frame protection, which is in 802.11w. However, 802.11i is a huge security suite, allowing for use of AES, an encryption standard, instead of WEP. “Nothing is mandated, so you can make yourself just as insecure as before,” he said. “Also, 802.11i typically requires a hardware upgrade on devices, such as handhelds and laptop cards, as well as access points. You can upgrade some with software, but others require hardware,” he said.

ISA’s SP100 standards committee defines procedures on how to implement wireless systems in the automation and control environment, focusing on the field level.

Project teams include co-existence, integration, interoperability, marketing, networking, physics of radio, technical RFP evaluation criteria (TREC), SP100.11, SP100.14, use case, and user’s guide. The wireless environment includes: the definition of wireless, radio frequencies (starting point), vibration, temperature, humidity, EMC, interoperability, coexistence with existing systems, and physical equipment location.