# How to Overcome Barriers to Wireless Adoption

 *By Adrienne Lutovsky, Staff Writer, ProSoft Technology*

Is wireless better or worse than a wired network? The answer is neither; it’s different. A plethora of wireless technologies exist to suit a variety of users. Is it for every application? No. But for many, wireless can be more flexible, versatile, and cost effective than wired networks. Yet, questions regarding security, reliability, and capacity of wireless continue to prevent conservative end users from reaping its benefits. Can these be overcome?

**No. 1: Security**

Security is the first topic to arise when discussing wireless in a plant network and the decision to deploy is often not one made in isolation. Plant engineers want to ensure uninterrupted production, and that security measures are in place to protect their process and plant floor equipment. IT engineers want to ensure that systems deployed in the plant co-exist well with networks in the rest of the organization and that nothing compromises the security of corporate information. Though different, the concerns of both the plant-floor engineer and the IT engineer are of high importance.

Today, the mechanisms are in place for industrial wireless systems to address the issues of both stakeholders. However, understanding what capabilities exist in wireless networking devices and how to utilize them for the betterment of the operation is not always appreciated. Modern encryption techniques can be utilized

to avoid someone interpreting your data maliciously. Filtering and strong authentication allow only authorized devices on the network. The mechanisms that are relied upon by the US government for transferring secret information are present in today's industrial wireless devices, and address many of the concerns of security of information, assets, and reliability of processes.

So, do not view the discussion on security for a plant network as one in which IT engineers and plant engineers have competing interests. Instead, acknowledge that each has their own experiences. Plant engineers have depth of experience in 24/7 reliability and the role reliability plays when deploying automation networks. IT engineers have depth of experience in co-existence of multiple systems and network management. The two can complement each other if cooperation exists.

### *Getting IT Onboard*

Swallow the lump in your throat and engage IT from the get-go. IT has likely deployed wireless more pervasively throughout their networks and will want to incorporate their best practices, allocate frequencies to ensure coexistence with other networks, and potentially help plan which technologies will be used. If IT is not included in the process and you proceed with your system, they can and will shut you down.

Lean on your solution provider. They should understand the needs of both departments and can bridge this gap to find a common solution.

Open dialogue about the security measures that can be put in place to achieve the same level of security as they are accustomed to with the wired systems. Today, with the standards that are in place, a fully provisioned wireless system can lock down the network securely and satisfy enterprise requirements. Sometimes this involves getting around red tape.

For example, heavily regulated industries like Pharmaceutical must adhere to strict data collection specifications, so the IT departments are more sensitive to security concerns. It is important to be clear on what you need and what IT will need from you in order for them to feel comfortable with your technology decision.

### *I'm a control guy and now I've brought IT in on my system. So, who owns my network in the event of a system down? How quickly can it be handled? How quickly can it be diagnosed?*

This is where it gets tricky. We are control people. Relinquishing decisions about our processes is antipodal to our natures. Who controls the network often comes down to the policy that exists or is set in place. With wireless, the same rules of demarcation should apply as would with Ethernet. In some cases, IT owns anything connected to Ethernet. In some cases the plant floor will own anything producing output. Sometimes IT will be involved in the decision making process and frequency allocation, but the plant has responsibility for installation and maintenance of the system. In any case, what becomes important is that the line of demarcation be established upfront and that the selected wireless technology provides the

diagnostic tools to satisfy both of these stakeholders.

The tools for IT and the plant floor may differ. Having the appropriate tools for each is critical to prompt resolution. In the IT world, tools are based on Simple Network Management Protocol (SNMP), which is supported by some industrial radios. Higher level diagnostics may include OPC level data that can be used to integrate diagnostics into the control system.

Though policy varies from one organization to another, the trend seems to follow suit of wired Ethernet on the plant floor. Whether wired or wireless, when a line goes down at two in the morning, it is the plant manager whose phone rings.

Regardless of who owns the network, it is fair to say that troubleshooting a wireless network has a different process than with a wired Ethernet system. A wireless network is not tangible, for one. You cannot hold it in your hand. It can be affected by outside contamination, which can widen the scope when trying to isolate the root cause of a problem. This is why it is essential to have proper tools in place to monitor and diagnose your system. As with every other essential component in your system, have someone clearly identified who knows how to use these tools and understands the equipment. Select a vendor that can support you throughout your implementation and down the road, with the proper tools and training, technology selection, and technical support program. With these things in place, someone who is familiar with doing the diagnostics on a wired network can also diagnose the wireless network.

**No. 2: Capacity**

***How can I feel assured that a wireless system will meet my bandwidth requirements, especially down the road?***

First, do your homework upfront. Know your network demands, your goals, and the environment you are dealing with. What are the distances and speeds you require? Do you need mobile worker access? Is your application indoor or outdoor? Are there reflective surfaces? Moving, rotating, vibrating machinery? Be able to articulate what traffic your network is expected to support. There are many flavors of wireless, each suited for different applications.

Second, choose your service provider carefully. Work with an industrial grade technology from a vendor that can confidently determine what you need in your specific application, and can select a scalable solution to accommodate your growth. Select vendors with a strong understanding of your equipment and your process. Look for the right combination of diagnostic tools. Some vendors provide HMI integration tools using OPC to give you a visual overlay of your network. Verify if the company offers value-add services such as path studies and site audits. These are things to look for when specifying your projects.

Some applications, however, simply cannot be supported by wireless. For example, production lines using 1000 I/O points with millisecond scan rates. Wireless technologies today cannot deal with this level of capacity.

***How can I protect my network from interference if a neighboring facility installs its own wireless network?***

Be conscious of what else is in place. Think of IT as an asset. Utilize their domain expertise and build a maintenance program for monitoring the health of the system. A solid understanding of the necessary criteria can provide can provide the ability to anticipate wireless performance over time. IT can sniff the network periodically, monitor for new participants or other change in the wireless environment, measure outside interference, and ensure performance is not diminished.

However, even a perfectly implemented network with a well-laid plan for isolating interference is vulnerable to the ever-changing RF environment. You cannot know if a neighbor will move in and interfere with your network, but you can take precautions or adjust you applications later to limit impact.

Several precautionary options exist. To start, it is wise to choose a solution with flexible frequencies that can be changed if needed (802.11n has 24 channels in the 5GHz band). Another effective method is the use of directional antennas to strengthen the connection between radios and to reduce sensitivity to interference. Lining up directional antennas, however—particularly at farther distances—can be difficult. Advanced installation techniques such as these are often set in place during site surveys, performed by top tier technology providers.

**No. 3: Reliability**

***Is wireless less reliable than a wired system?***

The answer is no, it’s different. In the same way that a user would not run cable next to drives because of interference, wireless interference must be considered. Wireless simply requires different steps. Factors like line of sight and selection of radio, antenna and cable become important. Consider the specific performance features of these devices against your application.

In many cases, a wired system can be less reliable, particularly with moving equipment where slip-rings are used for communication. The nature of these applications subjects cable to continuous flexing, breakage, or degradation over time.

***Wireless has long been successful in SCADA, but control?***

In many cases, yes. In manufacturing, Ethernet is now widely used in control; and where there is Ethernet, wireless often follows. Some wireless devices are sophisticated enough to act as managed switches, providing intelligent packet filtering. Some support deterministic applications, and can provide a high level of flexibility, speed, precision and predictability. In these projects it is critical that the design and technology of the system be carefully planned and executed, working closely with your distributor specialists, integrators and solution providers.

Another battle is the classic, ‘perception is reliability’ cliché. Any person with a computer and internet service has experience with wireless, generally riddled with memories of crashing routers and resetting modems. Who wants to risk this in their plant? Today, wireless products exist that are far more robust and reliable for industrial environments than traditional consumer or even enterprise level technologies. There are new techniques and testing tools available to determine when the network is approaching failure, and user interfaces to provide real-time health information. There are repeatable technology management and procedural management systems that can be put in place to increase reliability.

Many real-world wireless applications have actually improved efficiency and reliability by trading their wires for antennas. Applications with moving equipment can dramatically reduce costs, downtime, and maintenance using wireless.

For example, Proctor & Gamble migrated to wireless specifically to improve reliability. In the plant, they replaced slip rings with a wireless network that was designed to optimize their existing EtherNet/IP network. They used an 802.11 solution on a 5GHz frequency in order to co-exist with an already saturated 2.4GHz band. They were able to meet performance requirements with determinism, experienced fewer dropped packets, had no downtime from communication errors, and ultimately received a strong buy-in from plant technicians.

Liberty Airport Systems of Ontario, Canada, designs custom runways lighting systems for commercial and government airfields. The reliability of these lighting systems is critical to facilitate aircraft movement, so downtime can translate into flights being delayed, cancelled, rerouted, or in worst case scenarios, an incursion. The primary fiber optic communication lines run underneath airfield runways, and in the event that they are damaged can shut down the entire runway. Liberty now uses wireless as the independent backup communication system for many of their installations in order to increase uptime and cut maintenance costs. In one installation, the fiber line was severed during construction, and the wireless backup system seamlessly carried on communication for a week while the fiber line was repaired.

## Conclusion

In the end, the keys to overcoming obstacles now and down the road begin with proper understanding, planning, and execution of your wireless network.

Wireless is not a “set it, forget it” solution. Audit your network. Engage with IT early on. Give them what they need to feel comfortable with the plan, and they will often help take care of the network.

With these things in place, users can enjoy the flexibility and versatility innate to wireless, and in many cases, reduce costs.

*For more information, please visit* www.prosoft-technology.com *[1].*

**Links:**
[1] http://www.prosoft-technology.com/