My personal experience of the 802.11bg (Wi-Fi) wireless band is decidedly jaundiced. As a reasonably experienced mobile user, I seldom achieve a level of wireless connectivity that I would consider even 'remotely robust'. But my opinion of wireless reliability is changing – fast.

Would you put a mission-critical network on wireless?

Graeme Bell, Managing Editor:
SA Instrumentation & Control

So would I consider running a mission-critical process control system on an 802.11bg wireless network? Until recently, my response to this question was a definite, "No!" But then I attended *Honeywell Process Solutions*' User Group Conference 2006 (HUG).

After listening to what various technology specialists had to say on the matter, I have considerably softened my stance. Honeywell and its technology partners put forward a very convincing argument for the immediate implementation of wireless technology in mission-critical applications i.e. not some time in the future, but now, March 2007.

Why wireless?

Why would one even consider putting any part of an industrial network on a wireless framework? Honeywell suggests that there are a number of benefits to be achieved from the implementation of an all-wireless industrial control network. These include significant cost-savings, increased mobility and increased network reliability.

If you think that these are idealistic and unachievable dreams, read on.

Costs savings

Consider the potential cost savings of not having to run any cables to any field device in a plant. If the device was simply used for measurement e.g. a temperature, it could be powered by a battery with an operating life of 3 to 10 years (dependent on the measurement rate).

If the device did require power for control e.g. an actuator, all one would need do is to provide it with a power source… and that could be sourced from the nearest electrical panel. The control signals would be delivered to the device by the wireless network.

Of course the cynic in me has to wonder the validity of these potential savings. Think of the companies that expected massive savings from the installation of fieldbus networks, only to be caught up in a quagmire of immature and often conflicting network technologies. However, oil and gas giant, Repsol, has installed Honeywell's wireless technology on a 936 km fuel gas pipeline. The savings reported are not to be sneezed at:

- 37 percent lower installed cost than traditional instrumentation.
- 50 percent reduction in maintenance costs.

Honeywell also contends that considerable savings are possible by running not only critical control data on its wireless networks, but also 'normal' IT data, as found on normal corporate networks. More about how that is possible will follow later in this article.

Mobility

Imagine maintenance staff having data access to any device in a plant, from any location? With an 802.11 network, all the user requires is a device that has the ability to connect to a 'standard' wireless network. Examples of such devices include certain cellphones, PDAs and most laptop computers.

Increased reliability

Honeywell argues that a significant percentage of control system failures can be ascribed to cable faults. Logic would have it that the exclusion of a physical transmission medium substantially raises the reliability of a network. In the Repsol installation mentioned above, Honeywell reports that: "all data transmission faults caused by wiring, marshalling panels and junction boxes were eliminated and measurement reliability was greatly enhanced."

Why not wireless?

At HUG 2006, Honeywell co-opted ARC Advisory Group (arcweb.com) to present the results of its research into end-users' concerns about the industrial use of wireless networks:

Security and safety are critical

Honeywell rightfully argues that it is a false sense of security to believe that mission-critical data in a cable medium is necessarily safer than wireless, simply because it is constrained to a physical cable. Poorly protected (encrypted/firewalled/physical) data on Ethernet is considerably more dangerous than suitably encrypted wireless data.

Honeywell has partnered with Canadian cyber-security specialists, Byres Security (byressecurity.com) to produce an 'industrial-grade firewall'. CEO, Eric Byres, reports that: "The last five years has seen a significant upswing in industrial security hacking attempts. Currently there are between 400 and 500 industrial cyber security incidents occurring per year to Fortune500 companies in the US alone. There have been attacks against every single manufacturing sector. This problem is not unique to oil and gas, nuclear or utilities."

Byres proposes that the correct implementation of security procedures, data encryption, and network firewalling (using Byres' Tofino Industrial Security Solution, of course) will address all user concerns regarding the vulnerability of wireless networks.

"We guarantee our industrial-wireless solution will work"– Director Sales Support, Jean-Marie Alliet.

Network communications must be robust and reliable

Most Wi-Fi users have experienced significantly raised blood-pressure levels as they ponder the reason for their laptop's wireless connection 'randomly' dropping connections… usually at the most inopportune moment. My kingdom for an Ethernet cable?

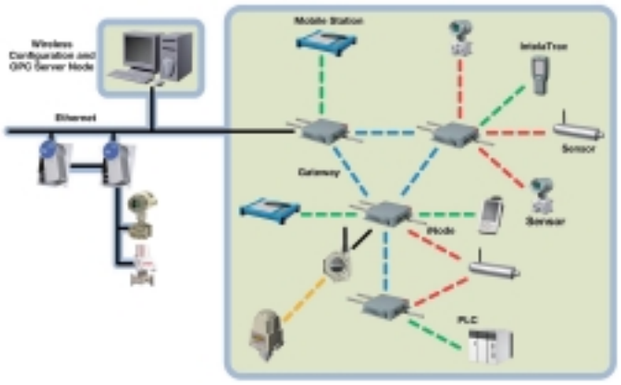
The most obvious indirect cause of our shared frustration is that all corporate, home and public wireless Wi-Fi networks operate in an already hugely overcrowded frequency band. This 'unlicensed' 2,4–2,5 GHz band is occupied by amongst others:

- Certain cordless phones.
- Some garage door openers.
- All Bluetooth devices.
- A veritable herd of other 'unlicensed' consumer devices.
- The common-or-garden variety microwave oven.

In mitigation of Wi-Fi, the reliability of any network is also determined by the skills of the respective network administrator. In the case of your home wireless network, who knows who set up your neighbour's wireless router… in all likelihood the neighbour concerned… someone most probably with the technical skills of a snail.

I asked the senior engineer (non-IT person) from one of Honeywell's clients about the time and specialist IT skills that they had needed to set up their first basic network, the very surprising reply I received was: "Uhm… none. Setup time was about 15 minutes."

Granted, not all installations are going to be that simple.



A typical wireless architecture employing Honeywell's iNode technology.

Despite this apparent simplicity of operation, Honeywell does contend that its 802.11 network topology is secure and robust enough for any application. Smart application of highly directional antennae is used to protect against interference, either from un-intentional or malicious sources.

The use of redundant network routes for every critical-data source is a key feature of the topology.

When I asked Honeywell director, Jean-Marie Alliet, in what environment Honeywell's network could NOT be installed, he replied, "There may be such an environment, but we have not found it. We already have an existing installation base of more than 35 million Honeywell wireless sensors."

"We guarantee that our wireless solution will work," he emphasised. "We have absolute faith in the reliability of this technology to convey the most sensitive mission-critical data."

Predictable power management in all environments for uptime

At the time of this article being authored, hardware vendors have still not agreed upon an electrical standard for the application of industrial wireless. There is a veritable plethora of contenders, including ISA SP100, Wireless HART, Wireless Industrial Network Alliance (WINA), and ZigBee.

Honeywell director, Dave Kaufman, is adamant that Honeywell's network topology is the only logical solution. Like other vendors' products, Honeywell's is a 'mesh' networks i.e. a large cloud/blanket is thrown over the plant, with devices relaying data back to the controllers. The problem with allowing battery powered devices to relay for each other, is that their power consumption fluctuates as the data rate fluctuates, making battery life unpredictable.

Honeywell overcomes this problem by not permitting sensors from acting as relay devices for other sensors' data. Rather, Honeywell employs the use of dedicated relay devices, called iNodes. iNodes are not powered by battery power, but by mains, making their fluctuating rate of power consumption irrelevant.

Kaufman argues that this ability to accurately determine battery life is key to the superiority of Honeywell's product.

One multi-functional and multi-speed wireless infrastructure investment to minimise installation, training, and security costs

Jean-Marie Alliet, contextualises: "The implementation of an industrial wireless network is not something that can be performed in isolation by the process control or instrumentation department. The role-out must be carefully co-ordinated between the engineering, production, security, asset control, accounting and IT departments.

Conclusion

Honeywell has invested considerable resources on what it clearly considers to be the next pre-eminent technological milestone. The company has more than 400 RF engineers that have produced more than 300 radio frequency (RF) patents that seek to boldly go where no critical network has gone before.

There is little doubt that wireless networking is on the march. Less-critical networks are already in abundance. It's only a matter of time before absolutely-critical applications start to appear. Once an electrical standard is agreed upon, users will have another reason to make the switch to wireless.

For more information about Honeywell's wireless solution, contact Honeywell Southern Africa on Tel: +27 (0)11 695 8000, hsa@honeywell.com or www.honeywell.com/ps/wireless

Graeme Bell
Managing editor, *SA Instrumentation & Control*
gbell@technews.co.za

About the author

Graeme Bell majored his under and post-graduate studies in commercial broadcasting engineering. He has an MBA, majoring in information management and currently holds the joint positions of Managing Editor of *SA Instrumentation & Control*, and CIO (Chief Information Officer) of *Technews Publishing.*