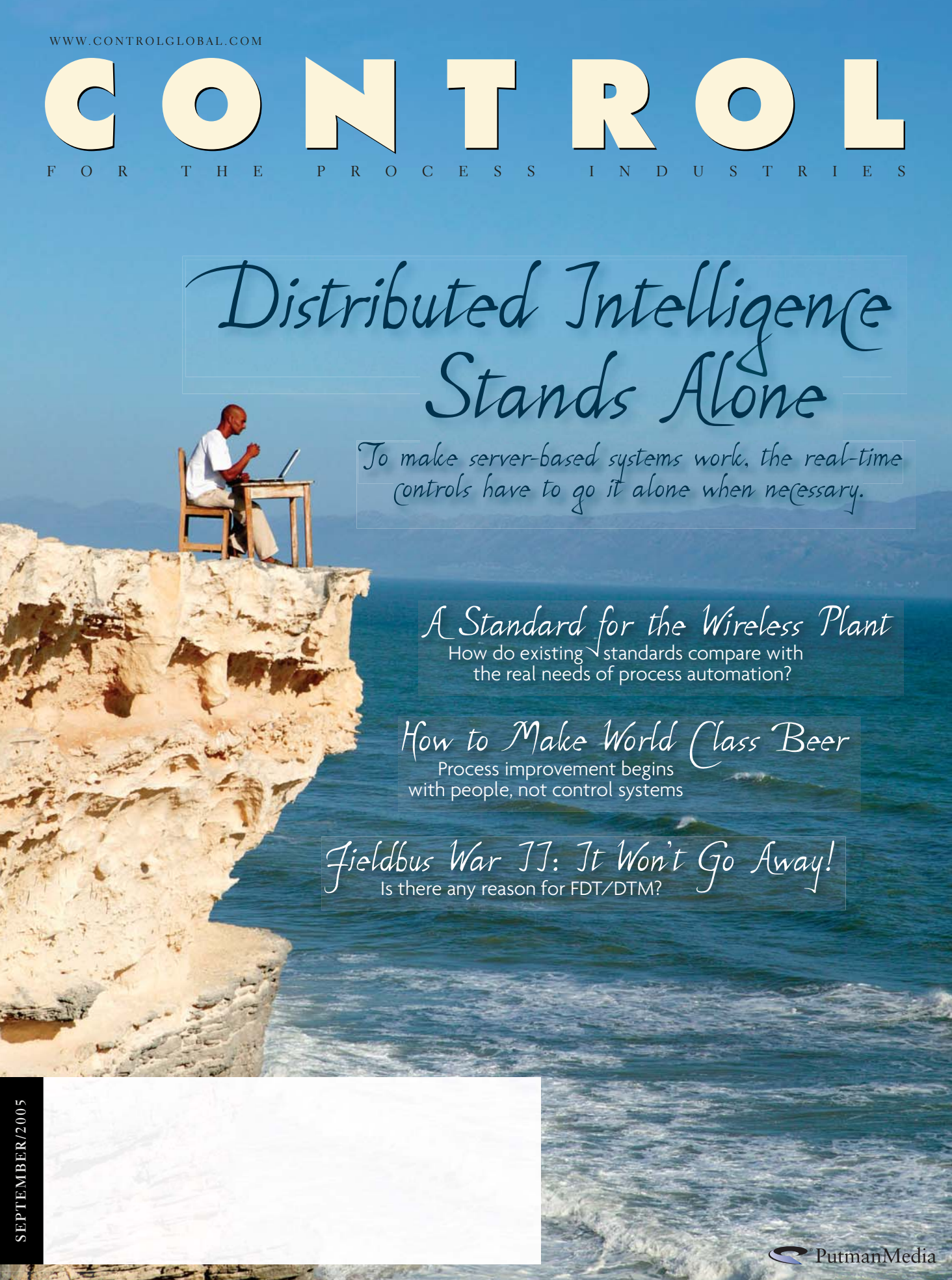
WWW.CONTROLGLOBAL.COM

CONTROL

FOR THE PROCESS INDUSTRIES



Distributed Intelligence Stands Alone

To make server-based systems work, the real-time controls have to go it alone when necessary.

A Standard for the Wireless Plant

How do existing standards compare with the real needs of process automation?

How to Make World Class Beer

Process improvement begins with people, not control systems

Fieldbus War II: It Won't Go Away!

Is there any reason for FDT/DTM?

SEPTEMBER/2005

PutmanMedia

USERS WANT AN INDUSTRIAL WIRELESS STANDARD

See how the existing standards measure up.

Walt Boyes, Editor in Chief

The call of wireless in industrial process plants is seductive. No wires, no wiring, lower cost, easy replacement and retrofit…it seems like it's too good to be true.

Well, it is too good to be true. Yes, companies are selling wireless products in industrial process applications, but this is still the very early days, and the old saw about the dancing bear applies. You know, "it's not that the bear dances well, but that it dances at all." Most of the applications currently in use are in inventory control or maintenance management systems, not process control. Nearly half the respondents to a recent CONTROL survey didn't believe wireless was robust enough for process control applications. Of course, over half of the respondents said they believed that eventually it would be.

Startups, FUD and vaporware

Fueled by the return of venture capital to the technology markets for the first time since the telecoms and Internet bubbles burst in 2000, many companies are staking their claim to be "the leading player in wireless sensor technology."

The buzz is biggest in building automation and home automation, because the numbers guys that work for the VCs can count the number of buildings and homes, and the potential number of sensors, and, as former Illinois Senator Everett Dirksen famously remarked, "Pretty soon, you're getting into real money." Even the U.S. Department of Defense and IBM are getting into the act. The DoD's dream is to be able to drop sensors like dustmotes across a battlefield, and be able to "see" a soldier's-eye-view. So it's also dropping money into wireless sensors. If the technology development in wireless sensors mirrors the last big thing DoD got hot about (RFID), we should see some striking improvements.

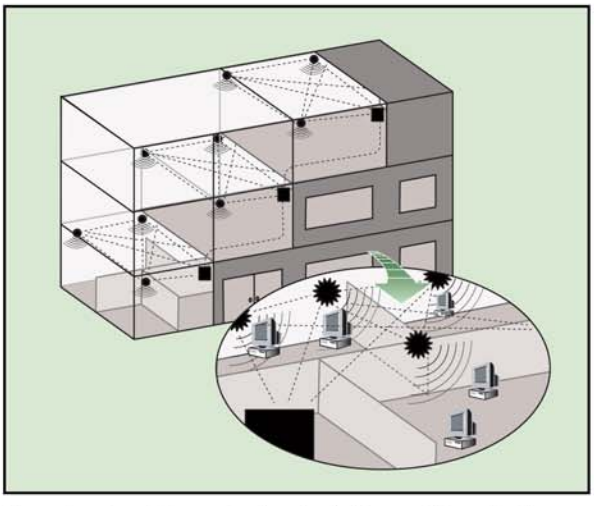
But, for the past three years, we've been trying to get people to discuss their existing wireless applications, and we've had little success. Either they aren't there, or they're not working well, or there is much more secrecy involved with wireless projects than any other process automation projects we know about.

"We are going to see the early adopters, the marginal projects, for a while yet," says Gerald Niemi, product manager for wireless at B&B Electronics. "Until standards settle down and products become fully industrially hardened, we won't see widespread use. This is still the Wild West."

One of the most developed set of applications is for energy management in large buildings and campus settings. Nels Tyring, the cutting-edge systems integrator and chairman of Automation Alliance Group (www.automationalliance.net), pointed us to a company named Obvius (www.obvius.com) with a wireless package aimed specifically at energy management systems, *and several large-scale systems installed*, including one at the University of Utah's Salt Lake campus. "They have been in the energy monitoring business for some time and have a very comprehensive package," Tyring said.

FIGURE 1.

MESHING WIRELESS NETWORKS



A mesh network is a set of router/retransmitters that form a self-organizing and self-repairing network

Bandwidth and Propagation: The Physics of Radio

Unlike all the other analog and digital communications methods currently in use in industrial process automation, wireless is not clearly easy to apply. Whether you are communicating in 4-20 mADC current, or HART (digital superimposed on analog 4-20), or via one of the other industrial fieldbus protocols, or via Ethernet, the fact is, you have a wire going from point A to point B, and if the wire is intact, the signal automatically goes from A to B, by definition. There are certainly problems with signal attenuation, especially over long distances, but these are straightforward engineering problems with recognized solutions.

Contrast this to radio, where signal transmission is inherently problematic, and a function of power, gain, interference, shielding, and even sunspots. A wireless signal is broadcast, not narrowly transmitted down a wire. It can interfere with other signals, and be interfered with in the same way. Like all RF energy, it can be shielded against, either deliberately, or more often inadvertently, by geographical features, buildings, and interior structures. These include steel beams, stairways, catwalks, and process vessels, all of which abound in process automation applications.

David Kaufman, an SP100 member from Honeywell (www.honeywell.com), says, "The operative issue is not how to make radio impervious to interference, but how to make error-checking and transmission protocols sufficiently robust, so expected signal losses don't cause errors in process control or data transmission."

Enter "mesh networking" (Figure 1). Widely confused with one of the IEEE wireless standards, Zigbee, mesh networking is not a standard, nor is it a protocol. It's actually a network topology. Mesh networks exist completely independent of radio, and chances are that you've used both of the largest existing mesh networks already today. They are, of course, the Internet and the telephone switching system. And if you are using VoIP for your telephone connection, you're using both mesh networks at the same time.

The idea behind a wireless mesh network is that redundancy is the savior of data loss. As with the famous Internet protocol, TCP/IP, mesh networks route signals between short distances to router-redirectors in a self-organizing, and self-healing fashion. That's the good news. The other piece of good news is that there is a standard: IEEE 802.15.4 or Zigbee, which uses the mesh network topology.

The bad news is that, like industrial Ethernet, there is Zigbee, and there is Zigbee, and just saying your device is Zigbee enabled doesn't mean it is interoperable.

Alphabet Soup: The Standards War

The situation is further complicated by the fact that there are several axes of interoperability, not one or two. Figure 2 shows the landscape of industrial bus networks, and notes that not all network protocols are useful for all devices and applications. Peter Fuhr, an SP100 member from Apprion (www.apprion.com), says, "This chart could be hideously more complicated 'cause there are over 120 different buses."

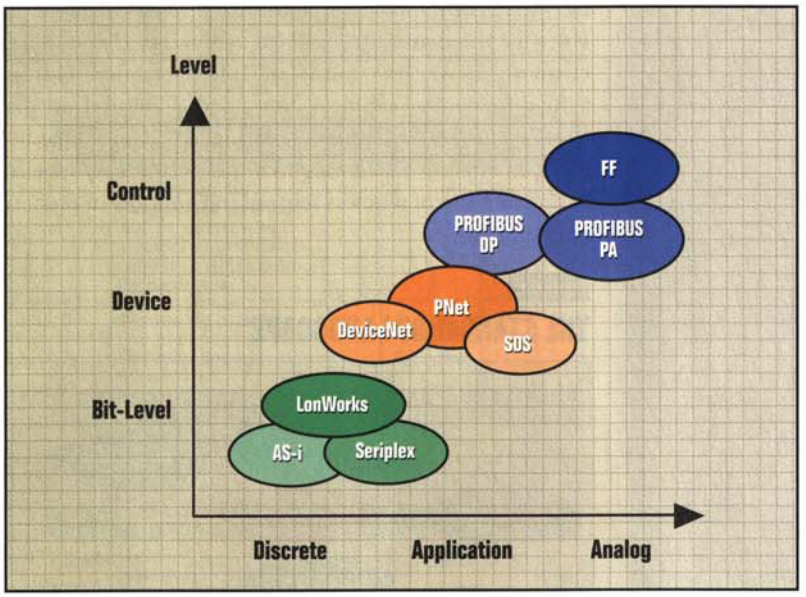
Now overlay the landscape of existing wireless networking protocols and standards, from Figure 3. Here we have more axes: power consumption, cost and complexity vs. data transmission rate.

As with industrial bus networks, there are turf wars, politics and other non-engineering related issues, which happen when many organizations are trying to develop standards in the same space. Figure 4 shows the intense competition in the wireless standards-making arena.

Unlike other industrial standards, the eventual industrial wireless standard must achieve total interoperability with the existing IEEE series of wireless standards, including WiFi, WiMax and others. That is going to be necessary because of the growing interpenetration of

FIGURE 2.

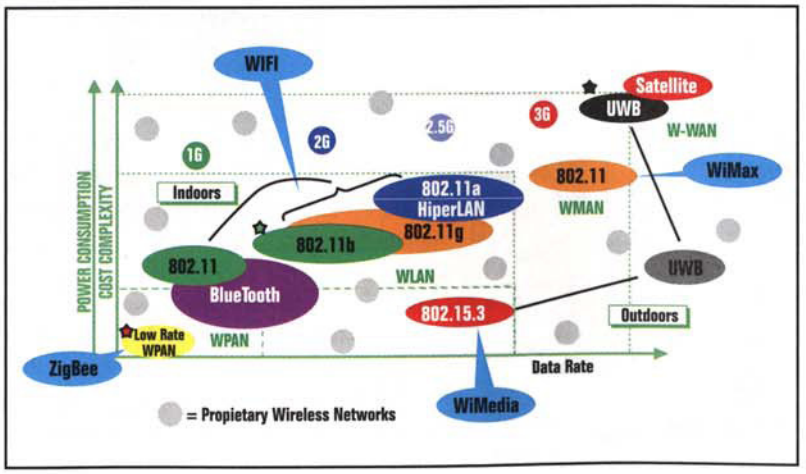
THE BUS NETWORK LANDSCAPE



Industrial bus networks are a multiheaded hydra.
Courtesy of SP100 and Apprion

FIGURE 3.

THE WIRELESS LANDSCAPE



A hodgepodge of mutually incompatible standards litters the landscape.
Courtesy of SP100 and Apprion

the plant-floor space and the enterprise, where the IEEE standards are ubiquitous.

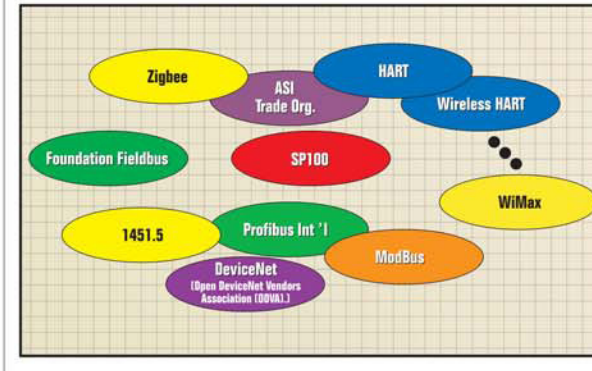
Drawing on the SP50 fieldbus standard experience, the SP100 committee doesn't want to create a situation in which, in the words of committee member Tom Phinney of Honeywell: "You only co-exist if you use my spec." It will be critical that any standard be absolutely non-proprietary.

SP100: Taming the Wireless Dragon

Under the leadership of Wayne Manges, from Oak Ridge National Laboratory, and Richard Sanders, from ExxonMobil, ISA's SP100 committee is creating a single industrial wireless standard for automation. The first deliverables for the committee will be a Wireless User Guide, currently in outline form, an Interoperability Guide, a Requirements Technical Note, and a Tutorial on the Physics of Radio. Eventually, the goal is a standard for industrial wireless networking that will permit easy specification and use of wireless sensors and controls in process automation.

FIGURE 4.

THE STANDARDS LANDSCAPE



The role of Standards, Wireless Organizations and Industrial Bus Organizations is not to confuse or constrain, but that happens anyway.

The SP100 committee will host a series of technical sessions at ISA 2005 in Chicago (currently scheduled for Thurs., Oct. 27) which will be "required attendance" for anybody wanting to get up to speed on the state of wireless in industrial automation.

What End-Users Want

It is already clear that users want what isn't yet available. Figure 5 shows a comparison between the requirements that the SP100 committee has identified and the existing wireless standards. Note that very few of the existing standards appear to be suitable to meet the SP100 requirements.

Clearly the SP100 committee has a tough and important job ahead.

FIGURE 5.

HOW THEY COMPARE

Sort Index	Requirement #	ISA-SP100 Requirement* Description	Wireless Protocol Standards				
			ISA-SP100	802.11g	802.11s	ZigBee (802.15.4)	WiMax
1		**Cost**					
2	1	Low Capital expense	4	4	4	4	0
3	2	Low Operational expense	4	4	4	4	4
4	3	Easy installation and maintenance	4	4	4	4	3
5	4	Power management	4	0	0	4	0
6		**Compatibility & Scalability**					
7	5	Interoperability -- Single Backbone for 802.11 and wireless sensors as well as co-existence with existing RF deployments	4	4	4	0	0
8	6	Worldwide usability	4	4	4	4	4
9	7	Capacity and scalability	4	4	4	1	3
10		**Security**					
11	8	Network security	4	4	4	2	2
12	9	Messaging security	4	4	4	1	0
13		**Performance**					
14	10	Reliable communications	4	2	2	2	3
15	11	Adequate Reporting rates	4	3	3	1	0
16	12	Suitable for closed-loop control	4	1	1	0	0
17	13	Support peer-to-peer control in the field	4	0	0	4	0
18		**Local field device access**					
19	14	Local field device access by handhelds/ portable devices	4	2	2	2	2
20		**Quality of Service (QoS)**					
21	15	QoS (Timeliness, Delivery Ordering, Recovery Action)	4	2	2	2	2
			60	42	42	35	23

*Requirements based on Voice of the Customer studies

Ranking 0-4; where 0 = no compliance

where 1 = 25% compliance
where 2 = 50% compliance
where 3 = 75% compliance
where 4 = 100% compliance

The major wireless standards, and how they rate as industrial standards. Courtesy of SP100 and Honeywell Inc.