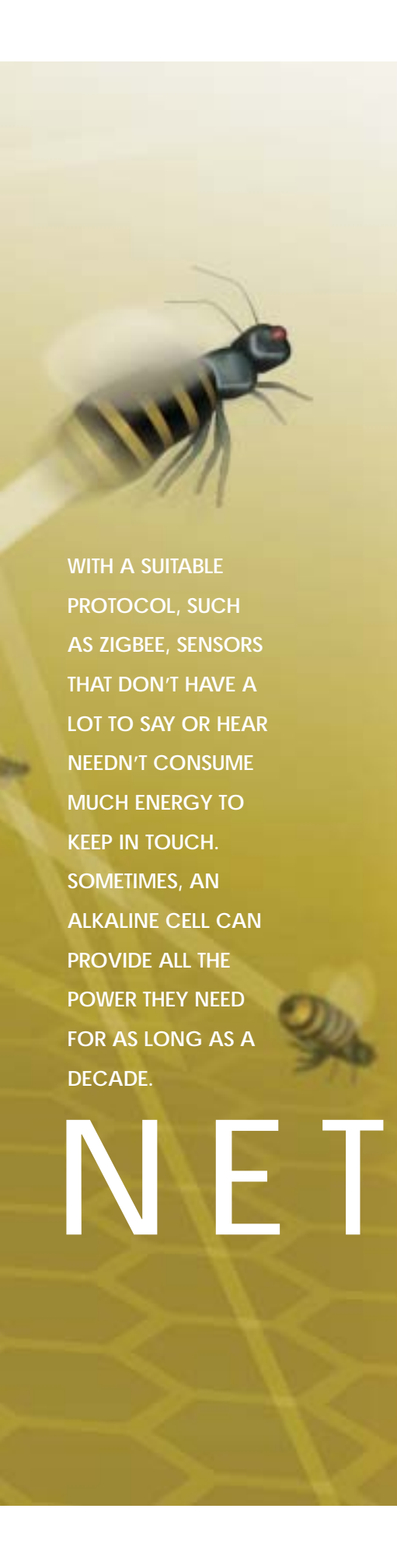


SIMPLE



WITH A SUITABLE
PROTOCOL, SUCH
AS ZIGBEE, SENSORS
THAT DON'T HAVE A
LOT TO SAY OR HEAR
NEEDN'T CONSUME
MUCH ENERGY TO
KEEP IN TOUCH.
SOMETIMES, AN
ALKALINE CELL CAN
PROVIDE ALL THE
POWER THEY NEED
FOR AS LONG AS A
DECADE.

NET

WORKS

will free many
sensors from wires

The folks at the ZigBee Alliance, the industry organization driving ZigBee WPAN (wireless-personal-area-networking) technology, mean it when they say that they've learned valuable lessons from the miscues of the proponents of another such technology: Bluetooth. Bluetooth is now well-established and is here for the long haul—at least in the narrowly targeted market niche of wireless headsets for cell phones and portable entertainment devices. However, its advocates' early misadventures with creeping elegance almost sank the standard while it was still in its formative stages and certainly delayed its widespread deployment. The lesson: In this era of wireless everything, trying to be all things to all people is an almost-sure-fire recipe for failure.

ZigBee's creators based it on the IEEE 802.15.4 wireless-communication standard and named it for the zigzag "dance" that honeybees use to communicate the location and distance of sources of nectar. It is a technology that knows its place. It targets sensors, but not even all sensors—just low-speed devices that need to send data no more often than about once per second. There are several reasons for this focus: If a sensor is to be wireless, eliminating the signal wiring doesn't accomplish much if power wiring is still necessary. So, at least initially, most ZigBee sensors will be battery-powered. Most sensors are small, suggesting that battery-powered versions must not be much larg-

er. Therefore, the batteries need to be small, and small batteries store only modest amounts of energy.

To achieve acceptable battery life, the sensors and their communication circuits must therefore use power sparingly. The most straightforward way to achieve this goal is to minimize the duty cycle—in this case, the percentage of time that a device is on the air. When not communicating, the device is in a low-power sleep mode. Most sensors generate messages that last only a few milliseconds at 802.15.4's data rate of 250 kbps at 2.4 to approximately 2.48 GHz. The rates are 40 and 20 kbps, respectively, at 902 to 928 MHz and 868 to 870 MHz. Because the

AT A GLANCE

■ ZigBee is a low-power, relatively low-speed wireless-personal-area-networking technology that aims at sensors.

■ By not attempting to be all things to all people, ZigBee is getting a warm reception.

■ Alkaline batteries will power most initial ZigBee devices. However, energy harvesting, which scavenges small amounts of energy from the environment, such as from light and vibration, offers the hope of eliminating batteries from some ZigBee applications.

■ ZigBee will make slow and steady inroads into industrial applications. A conservative approach is warranted, because demonstrating the reliability of a low-speed protocol takes time.

transition from sleep mode to data transmission takes approximately 15 msec, a sensor that sends, on average, one message per second usually operates at a duty cycle of 2% or less in the 2.4-GHz band and little more in the 868- and 915-MHz bands. Many sensors send messages much less often. For these sensors, the duty cycle is so low that the battery life can essentially equal the battery's shelf life: as long as 10 years for alkaline cells.

SOLID RATIONALE

The rationale for having a standard for networks of wireless sensors is a lot more serious than, "Everything is going wireless these days, so why not sensors?" Many applications involve large numbers of sensors. In such cases, the cost of mounting and wiring the sensors can greatly exceed the cost of the sensors themselves. Of course, ZigBee doesn't address the not entirely facetious issue of having sensors fly unaided to and then perch at the spot where you'd like them mounted, so part of the cost of sensor installation remains even with wireless sensors.

ZigBee targets a wide range of building-automation, industrial, medical, and residential-control and -monitoring appli-

cations. Applications that require IEEE 802.15.4's interoperability, RF characteristics, or both can benefit from ZigBee. Examples include: lighting controls; remote reading of electric, gas, and water meters; wireless smoke- and carbon-monoxide detectors; HVAC (heating, ventilating, and air-conditioning) and environmental controls; home security, intrusion, and motion detectors; blind, drapery, and shade controls; medical sensing and monitoring; universal remote control of set-top boxes that include home-control functions; and industrial and building automation. The first ZigBee products—for home-control, -safety, and -security applications—should appear in stores by midyear. Packaging for these products will prominently display the ZigBee logo (Figure 1).

The ZigBee specification overlays network-, security-, application-framework-, and application-profile layers atop 802.15.4's PHY (physical) and MAC (media-access-control) layers (Figure 2). The 802.15.4 standard's 2.4-GHz version is usable in unlicensed bands worldwide. It specifies O-QPSK (offset-quadrature-phase-shift-keying) modulation with half-sine pulse shaping, which is equivalent to MSK (minimum-shift keying). Each symbol carries 2 bits, channel spacing is 5 MHz, and there can be as many as 16 channels. Although devices do not frequency-hop among the chan-

ZIGBEE DOESN'T ADDRESS THE NOT ENTIRELY FACETIOUS ISSUE OF HAVING SENSORS FLY UNAIDED TO AND THEN PERCH AT THE SPOT WHERE YOU'D LIKE THEM MOUNTED.

nels, selecting channels can often optimize reception. To minimize interference among the networked devices and—in conjunction with other techniques—to enhance data security, the 2.4-GHz version also uses 2M-chip/sec DSSS (direct-sequence-spread-spectrum) coding. The less-than-1-GHz versions use BPSK



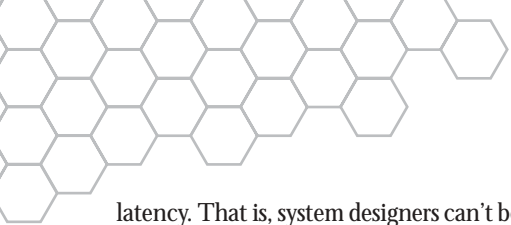
Figure 1 Like the standard it represents, the easily recognized ZigBee logo presents a simple, straightforward message to the customer. This version appears on the packages of consumer products that operate in the 2.4-GHz band. Versions also exist for products that operate in the less-than-1-GHz bands (courtesy ZigBee Alliance).

(bipolar phase-shift keying) with root-raised-cosine pulse shaping and, in the 915-MHz version, 2-MHz channel spacing. (The 868-MHz band has room for only one channel.) BPSK transmits only 1 bit per symbol. In the 868-MHz (largely European) and the 915-MHz (western hemisphere plus Australian) versions, respectively, the data rates are 20 and 40 kbps, and the DSSS chip rates are 300k and 600k chips/sec.

In all three bands, the 802.15.4 MAC layer uses CSMA/CA (carrier-sense multiple access with collision avoidance)—fundamentally the same mechanism that Ethernet uses. A device that wants to transmit wakes from sleep mode and first listens for activity on its channel. If it detects activity, it goes back to sleep for a random interval and then reawakens and again listens for activity. If it hears none, it sends its message. Of course, two or more devices can be listening simultaneously—in preparation for sending data. Several of them might incorrectly conclude that the coast is clear and begin transmitting at the same time.

MESSAGE GETS THROUGH

According to ZigBee Alliance members, because of the DSSS coding, the chances are good that the messages will get through despite the interfering transmissions. But if a sender does not receive an acknowledgment, it goes back to sleep for a random period and then tries again to send its message. The obvious problem with CSMA/CA is its nondeterministic



latency. That is, system designers can't be certain how long any message will take to reach its intended recipient. However, as Ethernet proved decades ago, when it was much slower than it is today, the scheme works admirably in many common applications. Also, the longer you can wait for a response, the greater the likelihood that the system can meet your needs.

For those who must have deterministic latency, however, the IEEE standard provides two additional mechanisms that together guarantee it within a tight tolerance. Beacons are special messages that are permitted in certain ZigBee network topologies. Beacons wake up client devices, which listen for their address and go back to sleep if they don't receive it.

It is possible to designate times, separated by multiples of 15.38 msec to a maximum of 252 sec, when the devices must listen for beacons. A beacon can announce a superframe, another kind of special message, which provides 16 time slots between beacons. During these slots, designated devices receive contention-free network access.

OVER-THE-AIR SOFTWARE DOWNLOAD IN WIRELESS-SENSOR NETWORKS

By Larry Friedman, Texas Instruments

A characteristic of wireless-sensor networks is their lack of physical connectivity (wiring) between the sensor/actuator array and the network. Although the absence of wires simplifies placing hardware in hard-to-reach locations, when software upgrades become necessary, you can't fall back on wires for downloading the new code. OAD (over-air downloading) solves this problem, but you must address several issues to successfully implement OAD. Texas Instruments supports OAD with the Chipcon Wireless OAD product.

In a layered transport architecture, such as ZigBee/802.15.4, support for a scheme such as OAD is a matter of writing an application. The layer at which this application exists is a design choice, and the choice has implications. For example, writing OAD support as a ZigBee application allows use of the entire stack as infrastructure to support multihop routing, thus eliminating the need for proximity between the source and the target. Using a MAC (media-access con-

trol)-layer application would sacrifice this network-routing support to reduce the size of the file-transfer-support code. All methods require a repository of some size to store the downloaded code.

OAD support must be fail-safe. It must be robust enough to survive transmission errors, interrupted file transfers, and interrupted enabling of the new code—that is, interrupted flashing of the new image. If any of these steps fail, the device's remaining software must be able to recover. The file transfer itself must also be secure.

To deal with interrupted transfers, the software must meet two conditions. First, the software entity that supports the transfer on the target must remain intact until the transfer succeeds. Second, you cannot expect the portion being transferred to operate until the transfer is complete. These two requirements together imply that the downloaded-code repository must store the transferred portion of the new code, and this por-

tion cannot disrupt the code that implements the transfer. If the code meets these conditions, the code supporting an interrupted transfer can retry the transfer at its next opportunity.

MITIGATING ERRORS

Frame-check sequences in the ZigBee stack mitigate transmission errors. Various layers each use these sequences to provide their own level of guaranteed-delivery support. In addition, you can apply a mechanism such as CRC (cyclic redundancy check) over the entire transferred file for a final check and to detect incomplete flashing of the newly downloaded code entity. Both ZigBee and the 802.15.4 MAC and PHY (physical) layers also support file-transfer security.

The file-upgrade-distribution architecture addresses how the target platform "knows" that an upgrade is necessary. TI's approach uses a managed client-server technique in which a management tool determines the code versions on each platform and assigns client and server roles

depending on the platform's location and the code's availability. The penetration of the new code increases as more target platforms receive the code. Each upgraded client can then become a server to another client. The management tool assigns these roles on the fly. This technique works because these networks, though often large, are well-defined and reasonably stable. A management tool makes sense in this environment.

AUTHOR'S BIOGRAPHY

Larry Friedman is a software-design engineer for low-power wireless devices at Texas Instruments Inc. He holds a bachelor's degree in psychology from Duke University (Durham, NC) and a PhD in psychology and computer science from the University of Maryland (College Park, MD). For the last 15 years, he has worked in design, development, and firmware architecture for small to midsized embedded systems and wired and wireless distributed-control and sensor/actuator platforms.



The ZigBee Alliance's slogan or position statement is "Wireless control that just works." From all indications available at this early date, ZigBee is living up to that slogan, but it took a lot of work and technology to make wireless control "just work." Version 1.0 of the ZigBee specification (Reference 1), which you can download at no charge from the Alliance Web site, runs 426 pages, and the PDF file fills almost 8 Mbytes. Moreover, the spec does not deal with the PHY and MAC issues that the 5-Mbyte, 679-pg IEEE 802.15.4-2003 standard covers (Reference 2). In other words, even though ZigBee is a well-focused, low-power, relatively low-speed protocol, its developers have invested a huge amount of effort to ensure that users find that it works without wheel-spinning or fuss.

One aspect of wireless-communication protocols that should concern all potential users is data security. Although you may wonder how much harm an interloper outside your house could do if he were able to, say, find out—or even change—the setting of your downstairs thermostat, the stakes are a lot higher in industrial and commercial applications. And, even in the home-thermostat example, the interloper might be able to cause very expensive mischief, such as frozen

- 8-BIT MICROCONTROLLER
- FULL PROTOCOL STACK: LESS THAN 32 KBYTES
- SIMPLE NODE-ONLY STACK: APPROXIMATELY 4 KBYTES
- COORDINATORS REQUIRE EXTRA RAM
 - NODE-DEVICE DATABASE
 - TRANSACTION TABLE
 - PAIRING TABLE

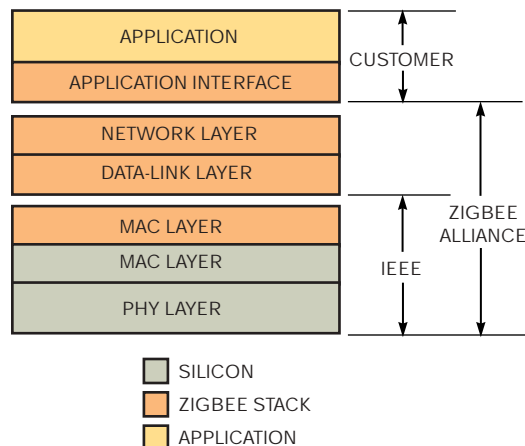


Figure 2 ZigBee is a layered protocol. IEEE standard 802.15.4 governs the bottom (green) layers. The ZigBee specification governs the middle (orange) layers. The customer controls the topmost application layer (gold). Orange denotes the layers that constitute the stack contained in ZigBee-platform ICs (courtesy ZigBee Alliance).

water pipes. ZigBee's DSSS coding provides a first level of security, but ZigBee also uses a security-toolbox approach to ensure reliable and secure networks. Access-control lists, packet-freshness timers, and 128-bit encryption based on the NIST (National Institute of Standards and Technology)-certified Ad-

vanced Encryption Standard help to protect data transmission and ZigBee networks themselves.

ZIGBEE PROFILES

A cornerstone of ZigBee is the profile, an example of which is home-control lighting. The initial version of this pro-

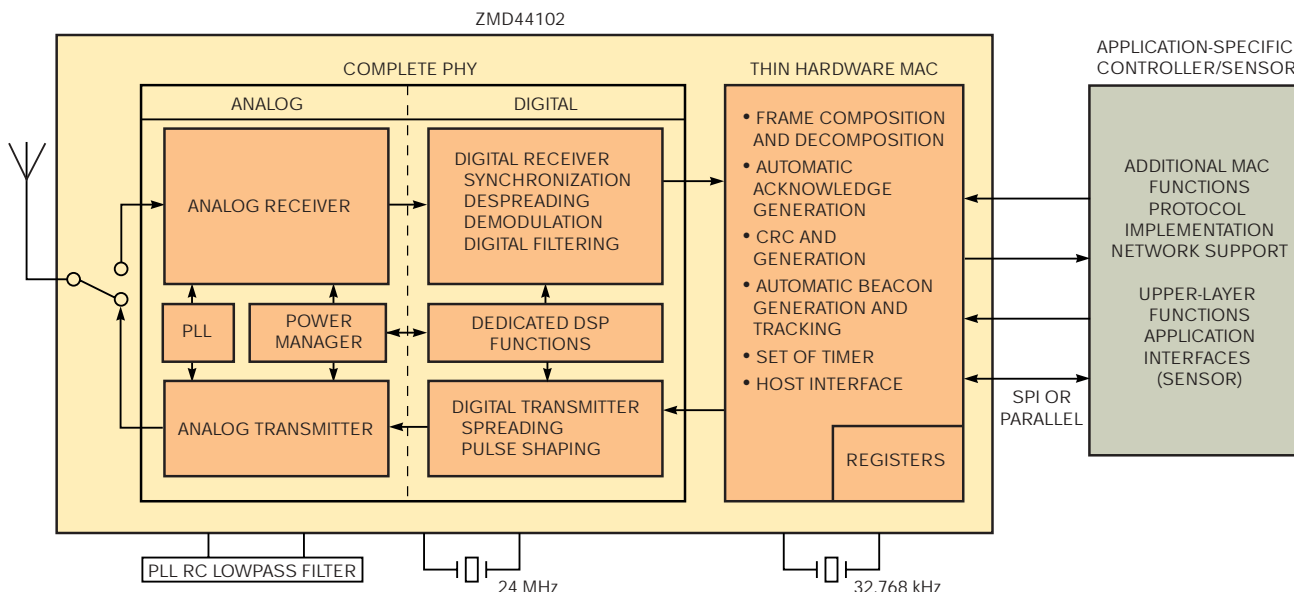


Figure 3 Though it applies to a less-than-1-GHz device, this platform is typical of single-chip ZigBee platforms. The ZigBee platform is on the left. The block at the right contains the application-specific functions (courtesy ZMD).



file permits a series of six device types to exchange control messages to form a wireless home-automation application. These devices exchange well-known messages to effect control, such as turning a lamp on or off, sending a light-sensor measurement to a lighting controller, or sending an alert message if an occupancy sensor detects movement. Another example is the device profile that defines actions common to ZigBee devices. For example, wireless networks rely on autonomous devices' ability to join a network and to discover other networked devices and the services they offer. The device profile supports device and service discovery.

The ZigBee specification allows device manufacturers to establish proprietary profiles that implement features you won't find in other manufacturers' products. The Alliance intends, however, that such proprietary features shouldn't prevent devices from different manufacturers from operating together in networks. That is, devices that implement proprietary profiles should still perform their basic functions even if other network devices lack features that the proprietary devices need to implement their unique capabilities.

The ZigBee-platform portion of a ZigBee device implements the RF- and baseband-communication functions. Although multichip ZigBee platforms are

currently common, expect the most common platform configurations to soon use one chip—not the identical design in all platforms, but a single chip from any of several suppliers (Figure 3). Different manufacturers' platform chips, which are expected to cost approximately \$5 each in production quantities, will differ in detail and depending on whether the intended use is at 2.4 GHz or at 868/915 MHz. Despite these differences, however, the ICs will perform all of the functions that are related to ZigBee but aren't specific to particular applications. Besides the RF functions, these chips will contain a processor and sufficient nonvolatile rewritable—that is, flash—memory to hold the ZigBee software stack.

Software, of course, plays a central role in ZigBee, and you can make a good case that no implementation of a software-dependent protocol is complete without a way of performing software upgrades. However, in a wireless environment, such upgrades present special problems that designers must work through in advance of deployment (see sidebar "Over-the-air software download in wireless-sensor networks").

Except in high-volume applications, for which it sometimes makes sense to integrate the application-specific functions with ZigBee-platform functions, expect the application-specific functions to reside on a second chip. An industry

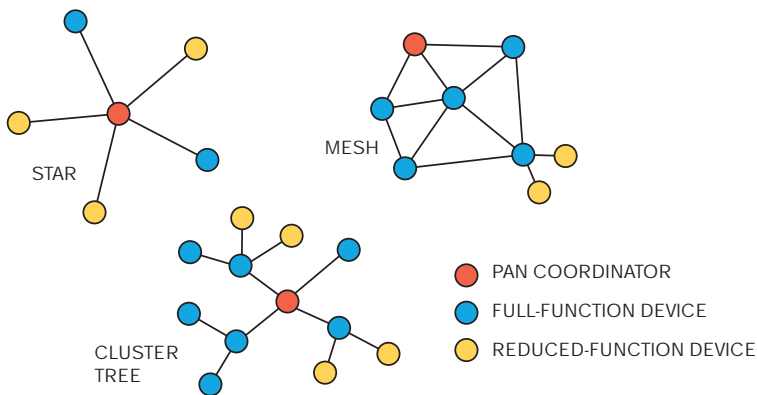


Figure 4 Although the mesh topology is most closely associated with ZigBee, the ZigBee specification offers two other alternatives and specifies which ZigBee features are available in each. Note that, in ZigBee, a message can make multiple hops to reach its destination (courtesy ZigBee Alliance).



is developing to provide ZigBee-platform modules, which contain the platform chip and additional circuitry, such as clock crystals, for example, to support that chip. Some of these modules provide features for prototyping the application-specific portion of the final device; others that target use in volume production lack prototyping features.

DIFFICULT QUESTION

A frequently asked question about ZigBee is: “What is the range of the transmissions?” Although the short answer is 10 to 100m, it is much easier to ask this question than to answer it. A thorough answer depends not only on whether the network operates at 2.4 GHz or below 1 GHz, but also on whether the networked devices are indoors or outside. Other factors include whether they operate at 0 dBm, which is the most common power and which ZigBee chips directly support, or at a higher power. The maximum is 20 dBm, but it requires an amplifier external to the ZigBee chip. The most important variable is how many hops the data makes before reaching its destination.

Although the 2.4-GHz band offers higher data rates than do the 868- and 915-MHz bands, advocates of the less-than-1-GHz frequency, such as ZMD (www.zmd.biz), say that transmission at the lower frequencies is more reliable because fewer users produce interference in the less-than-1-GHz bands and because problems with signal absorption and reflection are less severe at the lower frequencies. Therefore, the lower frequency devices can often operate at lower power.

The ZigBee NWK (network layer) supports star, tree, and mesh topologies (**Figure 4**). Network devices can relay messages from other network devices. In a star topology, a ZigBee coordinator controls the network. The coordinator initiates and maintains the network devices; all other devices are end devices, which directly communicate with the coordinator. In mesh and tree topologies, the coordinator starts the network and chooses certain key network parameters. ZigBee routers can extend the network. In tree networks, routers move data and control messages through the network using a hierarchical routing strategy. Tree networks can use beacon-orient-

MORE AT EDN.COM

For *EDN* Technical Editor Margery Conner's recent related article on wireless-sensor networks, go to www.edn.com/article/CA6313378.

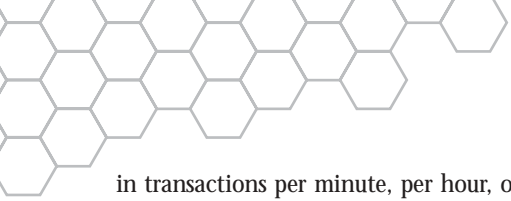
Go to www.edn.com/060413df and click on Feedback Loop to post a comment on this article.

ed communication. Mesh networks allow full peer-to-peer communication.

Tracking assets during inventory is an interesting application in which ZigBee may be more useful than the technology usually associated with the application: RFID (radio-frequency identification). RFID tags are passive; they receive the energy they use to respond to a query from the RF signal that issues the query. The problem is that the device that sends the query must usually be no more than about 3m from the RFID tag that provides the response. If you are, say, trying to locate test instruments in a large R&D or manufacturing complex, this characteristic presents a Catch-22: It doesn't make much sense to have to know where an item is to find it! A ZigBee network, however, can track the locations of instruments throughout a large campus. Each instrument must have a ZigBee platform, which is more expensive than an RFID tag, but, within the first year, the labor savings during inventory or when the calibration lab must retrieve instruments for calibration might easily exceed the ZigBee platform's cost differential.

TORTOISE OVER HARE

ZigBee's progress in industrial applications probably won't set speed records, but the technology is likely to win the race over competing technologies in the same way that the fabled tortoise triumphed over the hare—slowly and steadily. For example, it will take a good while before ZigBee can demonstrate the “five-nines” (99.999%) uptime that many industrial applications require. A major reason that such demonstrations will take time is the protocol's low speed when users apply it as its developers intend. Transaction-based applications measure ZigBee's speed not in transactions per second but



in transactions per minute, per hour, or even per month. Moreover, in predicting the reliability of real-world applications, you must deal with statistics and probability. Thus, it can take many months to demonstrate with high confidence that an application is subject to no more than

IF LOCATING A ZIGBEE SENSOR IN JUST THE RIGHT SPOT REQUIRED EXTRAORDINARY EFFORT, USERS WOULD LIKELY POSTPONE BATTERY REPLACEMENT UNTIL THE BATTERY DIED AND CAUSED A POSSIBLY EXPENSIVE FAILURE.

one error per month. In the test community, the speed issue has led some to believe that validation protocols based on bit- or frame-error rates are inappropriate for ZigBee and that tests based on EVM (error-vector magnitude) will more quickly yield accurate answers. Still, the warm initial reception the industry has accorded to ZigBee technology is encouraging Alliance members. Developers downloaded more than 18,000 copies of the ZigBee specification in its first year after publication.

Another issue that enters the thinking of prospective ZigBee users in industry is ZigBee devices' dependence on batteries. ZigBee ICs that have the wherewithal to measure the state of charge of the batteries that supply their power and routines for sending alarm messages shortly before batteries need replacement are among those that development-tool suppliers provide for embedding in the ZigBee stack. Nevertheless, if locating a ZigBee sensor in just the right spot required extraordinary effort, users would likely postpone battery replacement until the battery died and caused a possibly expensive failure.

Several techniques for extending battery life or eliminating batteries come to mind. If you can embed more intelligence in the sensor so that it can—without consuming much energy—make data-dependent decisions independently without

involving remote system elements, you can reduce the sensor's need to communicate and reduce the need for much of the energy that communication uses. However, such smart sensors present not only a formidable hardware-design problem, but also significant software-design challenges (**Reference 3**).

A different approach involves getting small amounts of energy from the environment through a panoply of techniques known as energy harvesting (**Reference 4**). For example, in a well-lit factory or office, solar cells might power a ZigBee device. A ZigBee light switch might obtain its energy from the movement of the toggle and store it in an ultracapacitor. (Light switches that need no ac connections *do* make sense! They can reduce wiring costs and simplify changes in office layouts.) Perhaps manufacturers can harvest energy from the stray ac magnetic fields surrounding wires that deliver power to motors and office machines. And they can harvest energy from the vibrations of production machinery.^{EDN}

REFERENCES

- 1 ZigBee 1.0 specification-download request: www.zigbee.org/en/spec_download/download_request.asp.
- 2 IEEE 802.15.4-2003 standard: <http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>.
- 3 National Instruments, white paper, *The real issue limiting wireless-sensor networks*, 2006, <http://digital.ni.com/express.nsf/bycode/sensors>.
- 4 Conner, Margery, "Energy harvesters extract power from light, vibrations," *EDN*, Oct 27, 2005, pg 45, www.edn.com/article/CA6275407.
- 5 Conner, Margery, "Wireless-sensor networks find a fit in unlicensed band," *EDN*, March 16, 2006, pg 46, www.edn.com/article/CA6313378.

AUTHOR'S BIOGRAPHY

Contributing Technical Editor Dan Strassberg has covered test and measurement for EDN for nearly 19 years. In that role, he has often covered sensors and networks. He holds two degrees in electrical engineering—a bachelor's from Rensselaer Polytechnic Institute (Troy, NY) and a master's from the Massachusetts Institute of Technology (Cambridge).