 By Warren Webb, Technical Editor

LOW-RATE NETWORKS TAKE CONTROL: REST ASSURED

AS BUSINESSES STRIVE TO INCREASE EFFICIENCY AND REDUCE LABOR COSTS THROUGH AUTOMATION, LOW-DATA-RATE NETWORKS ARE POISED TO BECOME THE WORKHORSES OF THE WIRELESS WORLD.

At a glance.......................... **46**

For more information...... **50**

Although much recent design and media attention has focused on high-bandwidth, video-capable wireless networks, the market for low-cost, low-data-rate RF links promises to be even larger. Automating just a few of the multitude of repetitive system-control and data-gathering tasks in business and industrial environments will generate enormous savings. Although proprietary low-bandwidth networking products have been available for years, a new push to standardize protocols promises to reduce silicon cost through higher volumes and guarantee interoperability among device suppliers. As new products and standards emerge, these low-cost communication links should prove popular, because users get immediate savings without the need to install expensive and inflexible network cabling.

There are literally thousands of em-

AT A GLANCE

▷ Low-rate networks are poised to deliver enormous savings to industry and building management by replacing human data-collection and -control tasks.

▷ Wireless low-data-rate networks that continuously monitor and control distributed systems offer low-cost hardware and long battery life.

▷ The recent IEEE standard 802.15.4 defines the physical and media-access-control communications layers for short-range, low-data-rate networks.

▷ The ZigBee Alliance of more than 60 vendors promises to add the remaining network, security, and application layers to complete the new standard.

▷ Although proprietary communications protocols currently dominate, new standards promise designers lower costs and product interoperability.

bedded-system applications in which a reliable, low-bandwidth communications network provides acceptable performance and reduces cost. For example, building-automation systems can significantly trim energy costs by minimizing lighting, heating, and air-conditioning usage depending on temperature, area activity levels, and time of day. Industrial users are installing low-rate networks to monitor the condition of production machinery to eliminate unnecessary service calls or equipment replacement. Utility-service providers can save millions of dollars annually with automatic meter-reading equipment that enables load balancing, identifies circuit failures, and eliminates human involvement to activate, deactivate, and read remote metering devices. Access-control, medical-monitoring, and security systems also reduce labor costs with strategically placed wireless links.

Although individual parameters vary from application to application, several common design requirements characterize low-data-rate wireless networks. Most applications call for a large number of sensor or control nodes; therefore, simplified and low-cost hardware is essential. Because you can deploy network nodes in remote and inaccessible locations, a long battery life is also one of the primary objectives. Although low node cost translates into reduced processing resources and simplified software, users still expect secure and reliable data transfers in the harsh RF environments of many industrial applications. Low-rate networks must also be scalable and adaptable so that users can quickly and easily add or reconfigure nodes as conditions change.

As with their high-bandwidth counterparts, you can arrange low-rate networks in multiple configurations for optimum performance. For example, a point-to-point wireless bridge connects two endpoints and simply replaces a communication cable. You can use a point-to-point wireless link to connect a remote-control panel to a movable device, such as a robot, to eliminate the tethered cable. Many low-data-rate, point-to-point links incorporate low-cost transceivers at each end that translate a common standard communications protocol, such as RS-232. Another wireless-network format, point-to-multipoint, includes a central base station and multiple wireless nodes arranged in a star or hub-and-spoke pattern. Although they are considered high-bandwidth networks, Bluetooth and IEEE 802.11 variations are based on the point-to-multipoint model.

Mesh networks, a third wireless format, are low-power, multihop systems that process messages by passing packets from node to node until they reach their destination. Unlike a point-to-multipoint network node that filters out all packets except its own, a mesh-network node receives and retransmits packets addressed to other nodes. A multihop network operates much like the Internet and provides redundant communications paths from source to destination. If a path stops working due to hardware failure or interference, a mesh network automatically reroutes packets through an alternative path.

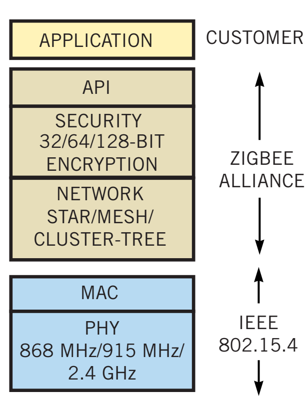


Figure 1 **ZigBee's communications layers, along with the IEEE 802.15.4 physical and media-access-control layers provide a complete, low-data-rate networking standard.**

In addition to the format, another wireless network distinction is based on range and application. A WPAN (wireless personal-area network) covers the 0 to 10m range, and its creators originally intended it to interconnect peripherals around an individual's workspace, as with Bluetooth. More recently, the WPAN definition has been extended to include any short-range communications link. Consequently, many low-data-rate networks fall into this category. As the range increases, a WLAN (wireless local-area network)—for instance, IEEE 802.11b—extends to approximately 100m, and a WWAN (wireless wide-area network) covers anything larger.

Although short-range wireless products often use proprietary protocols, the IEEE commissioned a task group to develop a standard for ultra-low-power, low-data-rate networks operating in the unlicensed, international frequency bands. The IEEE in May 2003 ratified the resulting standard, IEEE 802.15.4, which defines the PHY (physical-layer) and MAC (medium-access-control) sublayer specifications for low-rate devices communicating at 20 kbps in the 868-MHz band, 40 kbps in the 915-MHz band, and 250 kbps in the 2.4-GHz band. You can arrange networks, which include addressing for more than 65,000 nodes, in star or peer-to-peer topologies. Transmitters use DSSS (direct-sequence spread spectrum) with BPSK (binary phase-shift keying) in the less-than-1-GHz bands and O-QPSK (offset-quadrature phase-shift keying) at 2.4 GHz. The standard provides for 16 channels in the 2.4-GHz band, 10 channels in the 915-MHz band, and one channel in the 868-MHz band. The channel-access method is CSMA/CA (carrier-sense multiple access with collision avoidance). The specification describes two types of network nodes: an FFD (full-function device) that can perform any network duties and an RFD (reduced-function device) with limited resources and functions for cost-

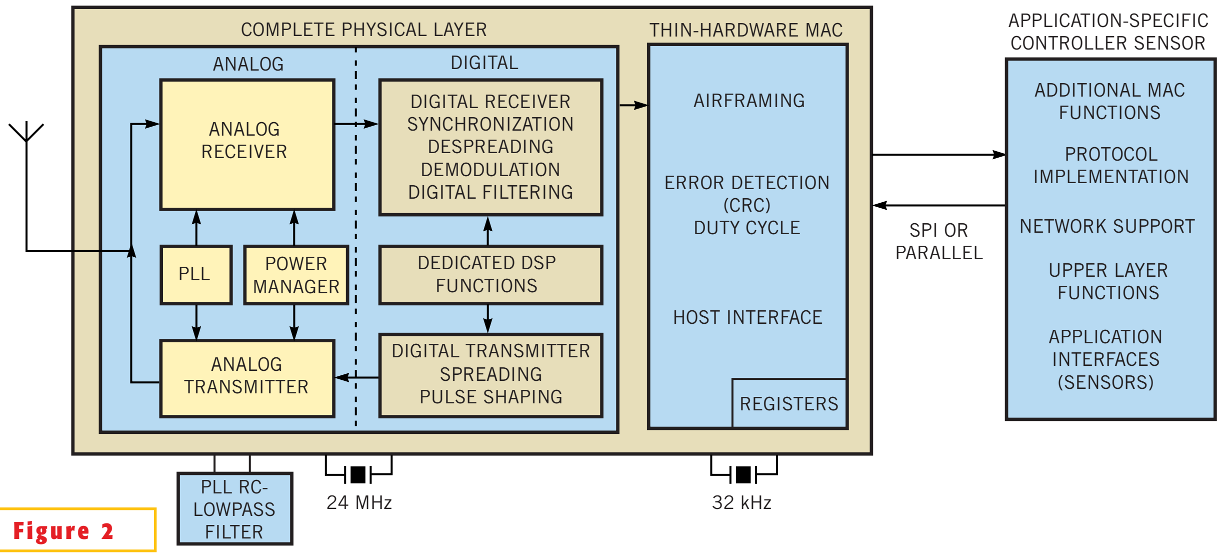


Figure 2

The ZMD44101 from ZMD is a less than 1-GHz CMOS transceiver with 40-kbps data rates and a standby current of less than 4 µA.

sensitive applications. You can download a free copy of the 679-pg standard at http://standards.ieee.org/getieee802.

ENTER ZIGBEE

With a global standard for the PHY and MAC layers in hand, the ZigBee Alliance is at work to define the remaining network, security, and application layers needed for widespread acceptance of any new wireless specification (**Figure 1**). Backed by Motorola, Honeywell, Samsung Electronics, Philips, Invensys, and Mitsubishi Electric, the ZigBee Alliance includes more than 60 member companies and expects to deliver the initial version of its specification by the end of 2004. In a role similar to the Wi-Fi Alliance for 802.11, the ZigBee Alliance plans to provide interoperability and conformance testing specifications, promote the ZigBee brand, and manage the evolution of the technology.

The ZigBee network layer is responsible for device discovery and network configuration. ZigBee allows star and mesh topologies along with a combination of the two, called cluster-tree networks. Each network must have at least one FFD, called the coordinator, to provide initialization, node management, and node-information storage. To minimize cost and power consumption, the remaining nodes can be the simple, battery-operated RFDs. ZigBee networks adapt to several data-transmission scenarios. For periodic data, such as with wireless sensors, nodes wake up at set times, transmit sampled data to the coordinator, and go back to sleep. A light switch delivers intermittent data and may connect and communicate with the network only when activated. Repetitive data applications, such as a mouse or keyboard peripheral, may use ZigBee's GTS (guaranteed-time-slot) capability to ensure communications without latency or contention. These network-layer data-delivery strategies allow system designers to trade communications frequency for battery life in RFD nodes. Very-low-duty cycles allow nodes with coin-type batteries to remain operational for years.

Although the basic IEEE 802.15.4 specification defines extensive network-security services, such as access control; 32-, 64-, and 128-bit data encryption; and frame integrity, ZigBee provides an extended toolbox for designers to customize security features for individual applications. The AES (Advanced Encryption Standard) calculations, which software or a dedicated AES engine can perform, contribute significantly to node power requirements. However, encryption functions execute only when packets are transmitting or receiving. Therefore, the average power remains low because of the low data rate.

Although critics argue that ZigBee serves the same short-range, PAN space as Bluetooth, the technologies' specifications differ greatly. Bluetooth uses frequency-hopping spread spectrum to combat interference and delivers data at a peak rate of about 720 kbps; ZigBee's

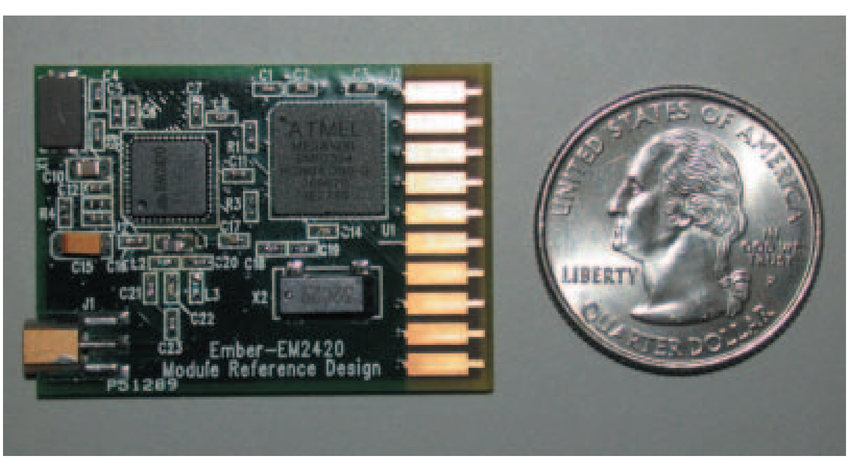


Figure 3 **Compatible with both ZigBee and Ember's software, the EM2420 RF transceiver reference design offers a link between proprietary and standards-based designs.**

maximum is 128 kbps. The basic Bluetooth protocol requires a complex communications stack consuming as much as 250 kbytes of system-memory resources, but a ZigBee controller requires less than 32 kbytes on an 8-bit controller. ZigBee devices can quickly attach, exchange information, detach, and then go to deep sleep to achieve a long battery life. The Bluetooth model assumes periodic battery charging similar to a cellular phone. Bluetooth networks require more than three seconds to add a new slave device; ZigBee requires only 30 msec. Finally, Bluetooth is limited to seven clients; ZigBee can handle thousands.

Figure 4 Crossbow Technology offers the MICAz RF transceiver, which bridges the gap between its extensive sensor-network products and the emerging ZigBee standard.

EARLY ADOPTERS

Because of the size of the potential market, hardware vendors are anticipating the ZigBee standard by introducing products that you can adjust to meet the final specification. For example, ZMD offers a system-on-chip transceiver designed to meet the PHY and MAC requirements of the IEEE 802.15.4 standard in silicon and implementing the ZigBee layers in the application-specific controller software (**Figure 2**). The ZMD44101 CMOS transceiver operates in the 868.3-MHz bands in Europe and the 902- to 928-MHz ISM (industrial, scientific, and medical) bands in the United States. This low-power, baseband transceiver delivers data rates reaching 40 kbps and incorporates DSSS technology to improve data transfers in hostile RF environments. With a typical standby current of less than 4 μA, the transceiver supports as many as 255 nodes in star or mesh network topology using the ZigBee network protocols.

Atmel recently announced a turnkey chip set for ZigBee designs. The AT86ZL3201 Z-Link controller integrates encryption hardware with an 8-bit RISC processor and data storage suitable for implementing ZigBee FFD nodes. Atmel's AT86RF210 Z-Link radio, an 868-MHz/902- to 928-MHz, 802.15.4- and ZigBee-compliant transceiver, has 10 channels at 40 kbps in the 915-MHz ISM band and one channel at 20 kbps in the European 868-MHz band. The air interface is DSSS, including spreading and despreading, using BPSK. The PHY includes receiver-energy detection, link-quality indication, and clear-channel assessment. The Z-Link MAC allows network association and disassociation, has an optional superframe structure with beacons for time synchronization, and has a GTS mechanism for high-priority communications. The radio supports as many as 65,000 nodes in star, cluster, or mesh networks with a range of 1 to 100m. Power consumption in sleep mode is 1 μA. Atmel prices its ZigBee chip set at $6.75 (100,000) for the radio, FFD controller, and 802.15.4 and ZigBee protocol stacks.

Another product aiming to bridge the gap between a proprietary product line and emerging standards is the EM2420 from Ember Corp. This 2.4-GHz RF transceiver is a low-cost, power-efficient IC targeting low-data-rate applications, such as industrial and building automation, defense and security, and environmental monitoring. When you combine it with an external microcontroller, the EM2420 complies with the IEEE 802.15.4 standard for short-range wireless communication. Ember can load this hardware platform with its proprietary EmberNet software to build self-organizing, self-healing mesh networks. Additionally, Ember designed this same hardware for future compatibility with the emerging ZigBee protocol. To ease development, Ember offers a communication-module reference design that integrates the EM2420 RF transceiver with an Atmel 8-bit AVR microcontroller (**Figure 3**). The reference design includes pc-board-layout techniques for the RF portion of the design. Ember also offers a complete development kit for the EM2420 for $13,950.

Crossbow Technology, one of the first wireless-sensor-network suppliers, recently introduced the MICAz, a remote-sensing module for enabling low-power, wireless, sensor networks (**Figure 4**). The MICAz includes an IEEE 802.15.4- and ZigBee-compliant RF transceiver operating in the 2.4- to 2.4835-GHz ISM band. The module's DSSS radio offers both 250-kbps data-transfer rates and programmable RF output power in the −10- to 0-dBm range. A hardware MAC provides 128-bit AES encryption and au-

FOR MORE INFORMATION...

For more information on products such as those discussed in this article, contact any of the following manufacturers directly, and please let them know you read about their products in *EDN*.

Atmel Corp
www.atmel.com

Crossbow Technology Inc
www.xbow.com

Ember Corp
www.ember.com

Honeywell
www.honeywell.com

Invensys
www.invensys.com

Mitsubishi Electric
www.mitsubishielectric.com

Motorola
www.motorola.com

Philips
www.semiconductors.philips.com

Samsung Electronics
www.samsung.com

TinyOS
www.tinyos.net

Wi-Fi Alliance
www.wi-fi.org

Zensys
www.zen-sys.com

ZigBee Alliance
www.zigbee.com

ZMD
www.zmd.de

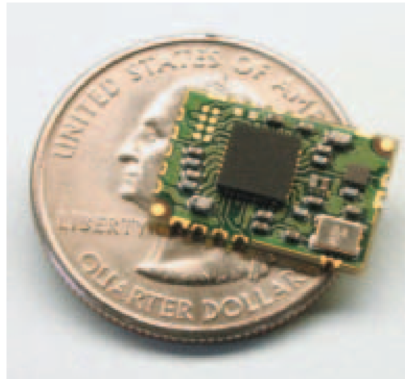


Figure 5 Even with new communications standards, proprietary, low-rate products, such as this Zensys transceiver, will continue to satisfy a large market segment.

thentication. The MICAz 51-pin expansion connector supports analog inputs, digital I/O, I²C, SPI, and UART interfaces. These interfaces make it easy to connect to a variety of external peripherals, including all of Crossbow's sensor boards, data-acquisition boards, and gateways. Sleep modes extend the life of the two AA batteries beyond one year. The MICAz module is available for $150 in low quantities.

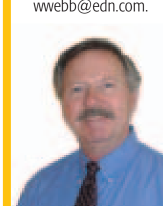
FREE NETWORK SOFTWARE

Many of Crossbow Technology's sensor modules feature TinyOS, an open-source operating system for wireless embedded-sensor networks. Applicable to both RF and MEMS (microelectromechanical-systems) communications technologies, TinyOS delivers real-time scheduling and extreme power-conservation algorithms in addition to bidirectional communications. TinyOS' component library includes network protocols, distributed services, sensor drivers, and data-acquisition tools that you can use as-is or modify for custom applications. With a potential memory footprint of less than 4 kbytes and open-source code, TinyOS is popular among resource-constrained sensor-network developers. TinyOS has been ported to more than a dozen platforms and numerous sensor boards. You can download the latest version of TinyOS at www.tinyos.net. A companion TinyDB project offers a query-processing system for extracting information from a network of TinyOS sensors.

Although the ZigBee standard promises to reduce the cost of transceivers, several vendors offer economical hardware for a variety of low-data-rate applications. Zensys delivers a family of Z-Wave modules that provide fully integrated radios that communicate in the unlicensed 868.42-MHz frequency band in Europe and 908.42 MHz in the United States (**Figure 5**). One of these products, the ZM1203, targets wireless control and monitoring applications, such as residential lightning and appliance control, energy management, access control, security, and building automation. The module employs Zensys' proprietary Z-Wave protocol, which features frame acknowledgment, retransmission, collision avoidance, frame-checksum check, and packet routing to ensure full network coverage. The ZM1203 module comes in a shielded enclosure containing the ZW0102 Z-Wave IC, a system crystal, and RF front-end circuitry. The ZW0102 includes the RF transceiver, an 8051 core, SRAM, flash memory for the Z-Wave protocol and user firmware storage, a triac controller, and a selection of hardware interfaces. Instead of a mounting connection, the ZM1203 uses castellation notches for attaching the module to an OEM-application pc board. The antenna is the only external component required for operation.

With potential applications in almost every industry, low-data-rate wireless technology offers network developers minimal-cost node hardware, flexible connection topologies, and long-term battery operation. Emerging standards, such as ZigBee, will enable volume production of node silicon and common software yielding even lower costs. Standards will also provide secure transmission protocols and guaranteed interoperability among certified product manufacturers. With approved standards and silicon manufacturers in place, you can expect to see explosive growth in low-rate wireless networking.□

You can reach Technical Editor Warren Webb at 1-858-513-3713, fax 1-858-486-3646, e-mail wwebb@edn.com.



TALK TO US

Post comments via TalkBack at the online version of this article at www.edn.com.