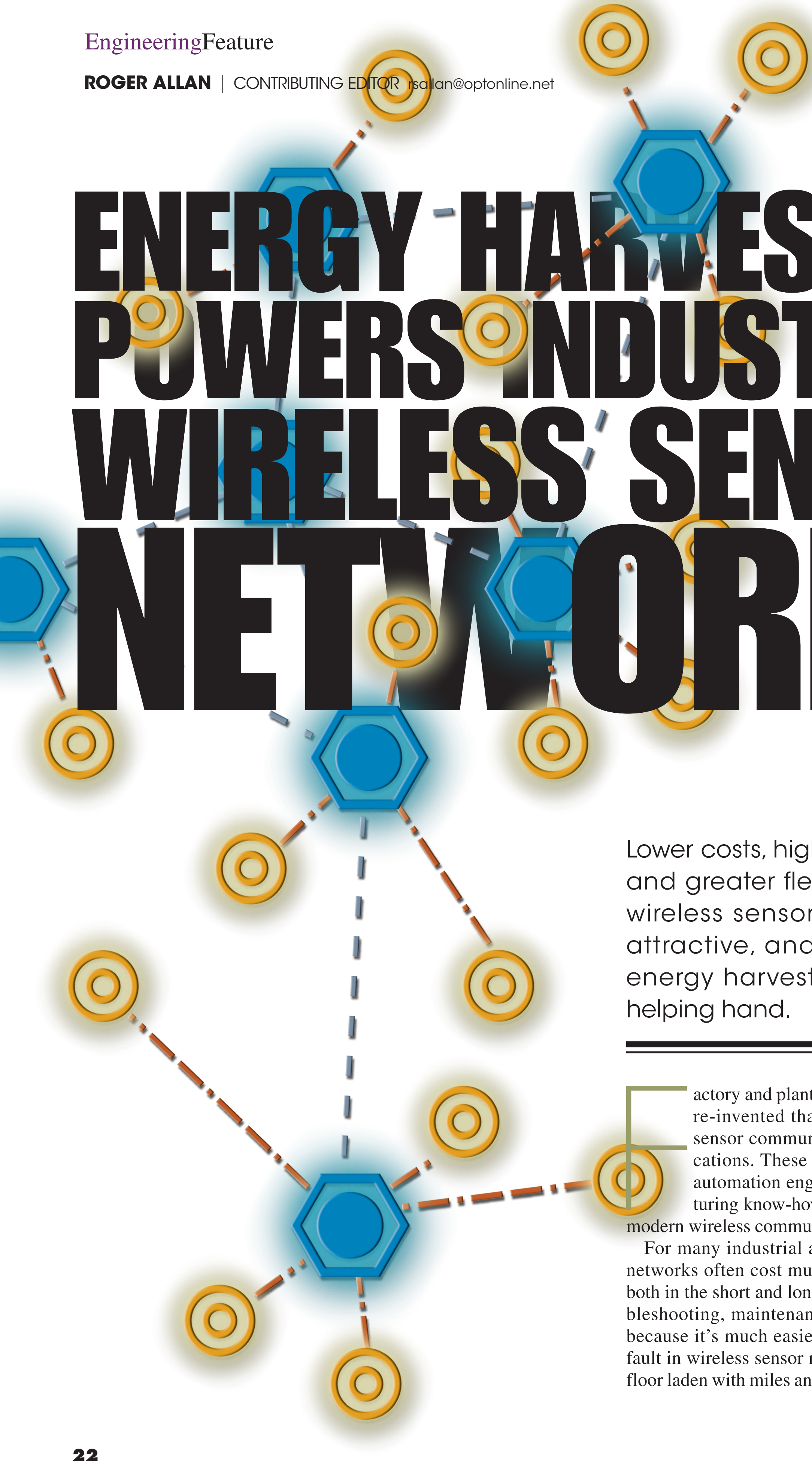
ROGER ALLAN | CONTRIBUTING EDITOR rsallan@optonline.net

ENERGY HARVESTING POWERS INDUSTRIAL WIRELESS SENSOR NETWORKS



Lower costs, high levels of reliability, and greater flexibility are making wireless sensor networking more attractive, and improvements in energy harvesting are lending a helping hand.

Factory and plant process automation are being re-invented thanks to advances in wireless sensor communications for industrial applications. These innovations are empowering automation engineers to blend old manufacturing know-how with the new capabilities of modern wireless communications.

For many industrial applications, wireless sensor networks often cost much less than wired solutions, both in the short and long terms, due to affiliated troubleshooting, maintenance, and repair issues. That's because it's much easier to track down a defect or a fault in wireless sensor networks than a wired factory floor laden with miles and miles of often buried wiring.

Wireless also is more flexible, allowing easier and quicker reconfiguration of a network to meet constantly changing plant needs for adjusting to newer product types and models.

Wireless sensor networks also can stream video via 3G and 4G network communications technologies due to their faster data transfers, which is very valuable in critical industrial sites that require around the clock monitoring and surveillance. Gas pipelines, video security systems, power facilities, water systems, and many other vital installations require immediate response to failures, tampering incidents, and accidents, and wireless sensor networks can save a company millions of dollars in fines for environmental violations, not to mention immediate control of environmental damages.

There's one caveat to using wireless communications networking in an industrial setting, though. The wide-scale availability of human-machine interface devices like smart phones and tablets poses potential security risks to wireless industrial automation if the correct security methods aren't employed *(see "How Safe Is Wireless Sensor Networking?" p. 28)*. Fortunately, many modern wireless sensor networking topologies and protocols feature built-in tools to minimize vulnerabilities.

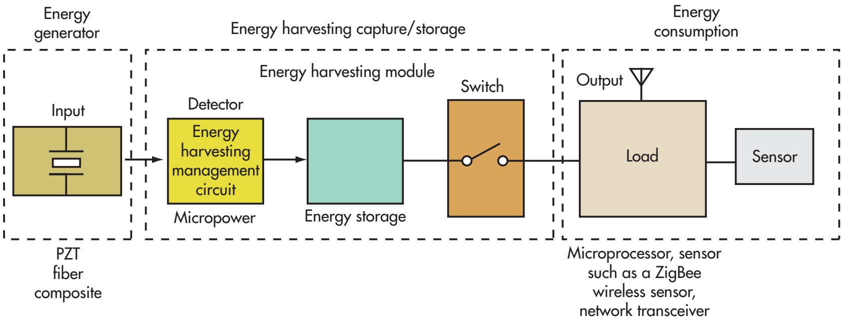
THE POWER ADVANTAGE

The benefits of wireless sensor networks go beyond these advantages. For example, wireless sensing and networking enables manufacturers to use low-power electronics, saving energy. Manufacturers can focus on the lowest possible power consumption, thanks to advances in communications protocols and the sensors and transceivers that power them.

Energy harvesting techniques save even more energy by working with modern IC functions. Some sensors, microcontrollers, power-management devices, and transceivers can operate from energy produced by a few degrees of heat, a small amount of mechanical motion, or some indoor lighting, all energy sources available within industrial plants *(Fig. 1)*.

These technologies minimize if not eliminate the use of battery power, leading to even lower energy consumption levels. Thermoelectric generators (TEGs), solar powered devices, mechanical motion sensors, and energy storage supercapacitors are all readily available.

"People are always complacent and somewhat happy about the use of battery power for wireless sensor networks," explains Tony Armstrong, director of product marketing for Linear Technology Corp. "But at the same time they're paying more attention to a battery's lifetime and are more concerned with energy harvesting techniques to minimize battery power consumption. What is important in wireless sensor networking is that there is enough energy available to do what needs to be done. We started this line of thinking back in 2009."



Energy generator
Energy harvesting capture/storage
Energy consumption
Energy harvesting module
Switch
Output
Input
Detector
Energy harvesting management circuit
Load
Sensor
Micropower
Energy storage
PZT fiber composite
Microprocessor, sensor such as a ZigBee wireless sensor, network transceiver

1. In a typical energy harvesting system, energy is generated from motion, a thermal source, a photoelectric source, or magnetic activity. This energy is then captured, stored, managed, and fed to a sensor and transmitter. *(courtesy of Advanced Linear Devices Inc.)*

THE INDUSTRY WEIGHS IN

The call for greater use of advanced communications technologies resonates well with the American Council for an Energy Efficient Economy (ACEEE). As indicated in its E125 report "A Defining Framework For Intelligent Efficiency," if industry as well as homeowners were to take greater advantage of currently available modern communications technologies like wireless networking, they could enable system efficiencies by about 12% to 22% and realize tens or hundreds of billions of dollars in energy savings and productivity gains.

According to the HART Communication Foundation, more than 8000 WirelessHART networks are currently installed in major manufacturing sites around the globe. The organization reports that tens of thousands of devices are at work in many process applications, including rotating equipment, pipeline monitoring, storage tank farms, automotive plants, and materials-handling facilities. Major companies such as Bayer, BASF, BP, Celanese, ConocoPhilips, Evonik, Pemex, Shell, and Statoil have developed networks and individual instruments at process manufacturing sites worldwide.

WirelessHART is based on proven international standards that include the HART Communication Protocol standard (IEC6158), EDDL (IEC61804-3), and IEEE802.15.4. The IEEE standard was adopted in 2007, based on work performed by Kris Pister at the University of California at Berkeley, and commercialized by his company Dust Networks in 1997 with the HART protocol. Dust Networks has since been acquired by Linear Technology Corp. Dust Networks widely popularized the term "mote" as a result of Pister's work.

WirelessHART is a wireless mesh network communication protocol for process automation applications. It adds wireless capabilities to the HART protocol while maintaining compatibility with existing HART devices, commands, and tools. Its three main elements are wireless field devices, gateways, and a network manager *(Fig. 2)*.

"We have literally set the standard for industrial process automation in oil and gas industries, chemical industries, wineries, breweries, to keep track of fluid levels, flow rates, machine vibrations, pressure, temperature, etc.," says Pister. "We have proven that wireless sensor networks are more reli-

able than wired ones and are less costly. Our strength is in ensuring that communications protocols are reliable and dissipate very low power levels."

Central to the HART protocol's success is the Time Synchronized Mesh Protocol (TSMP). The five key components of HART are time-synchronized communication, frequency hopping, automatic node joining and network formation, fully redundant mesh routing, and secure message transfer. TSMP networks also can self-organize. Every TSMP node has the intelligence to discover neighbors, measure RF signal strength, acquire synchronization and frequency hopping information, and then establish paths and links with neighbors.

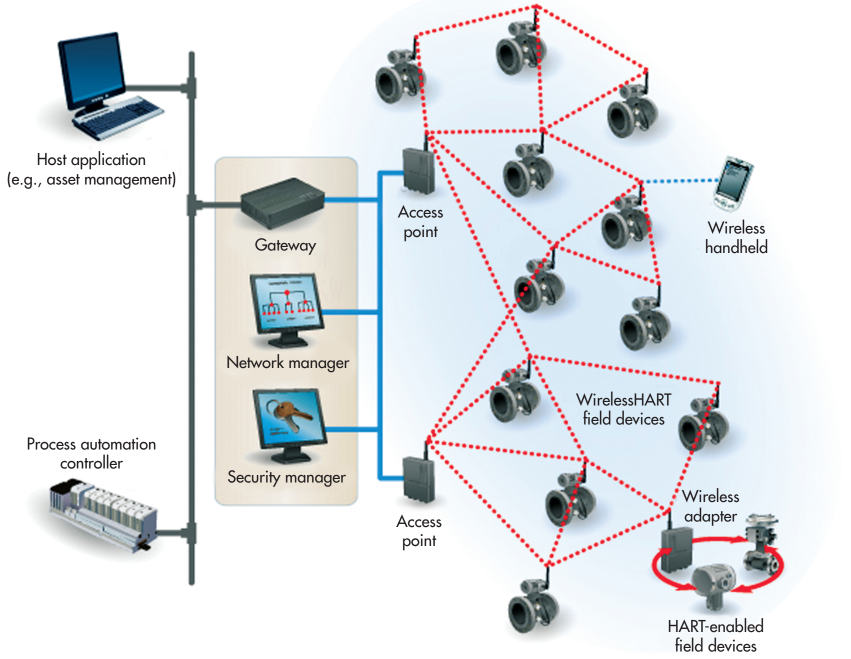
In TSMP, each communication window is known as a time slot. A series of time slots makes up a frame that repeats itself for the life of the network. Frame length is counted in slots and is a configurable parameter—in this way, a particular refresh rate is established for the network.

A shorter frame length increases the refresh rate, increasing effective bandwidth and power consumption. Conversely, a longer frame length decreases the refresh rate and decreases bandwidth and power consumption. A TSMP node can participate in multiple frames at once, allowing it to effectively have multiple refresh rates for different tasks *(Fig. 3)*. The TSMP packet structure with its temporal, frequency, and spatial diversity provides a robust protocol that stands up to real-world industrial challenges.

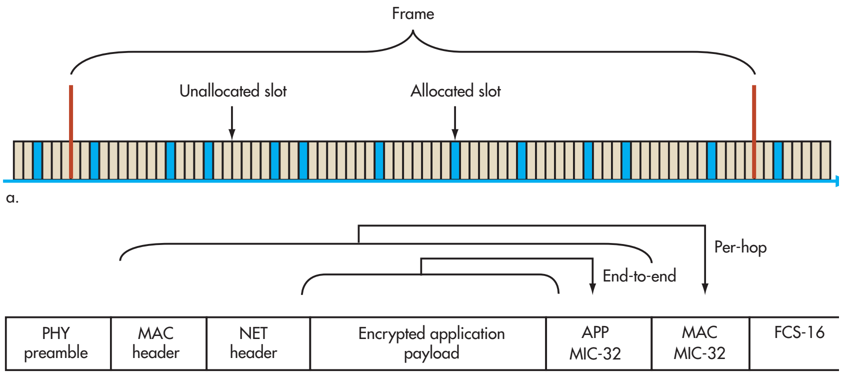
ELECTRIC MOTORS EVERYWHERE

Electric motors widely proliferate in industrial environments. Many experts estimate that the total cost of industrial electric motor ownership can be substantial, dissipating more than 90% of the plant's expended energy. Although modern electric motor efficiencies have been pushed up to 90% to 95%, optimizing a motor system's operation could save more than 20% of the energy expended. Wireless sensor networking for electric motor sensing, maintenance, and control is readily available.

Many wireless sensor networks take advantage of the mechanical energy (due to vibration) and thermal energy



2. WirelessHART mesh networks for process automation applications add wireless capabilities to the HART protocol while maintaining compatibility with existing HART devices, commands, and tools. Its three main elements include wireless field devices, gateways, and a network manager. *(courtesy of Dust Networks Inc.)*



Packet section	Description
PHY preamble	Preamble, start of frame delimiter, and length
MAC header	Per-hop addressing and timing information
NET header	End-to-end addressing and routing information
App payload	Encrypted application payload, packet-type dependent
APP MIC-32	End-to-end message integrity code for application data and nonce (32 bits)
MAC MIC-32	Per-hop message integrity code for the entire packet (32 bits)
FCS-16	Frame checksum for the entire packet (16 bits) per 802.15.4

b.

3. The Dust Networks Time Synchronized Mesh Protocol (TSMP) node can participate in multiple frames at once, allowing it to effectively have multiple refresh rates for different tasks (a). The TSMP packet structure with its temporal, frequency, and spatial diversity provides a robust protocol that stands up to real-world industrial challenges (b). *(courtesy of Dust Networks).*

4. EnOcean's ESK 300 version 1 868-MHz wireless development kit is designed to demonstrate energy harvesting and ultra-low-power radio technology. It comes with two electromechanical pushbutton generators for switches and a solar-powered temperature sensor. *(courtesy of EnOcean)*

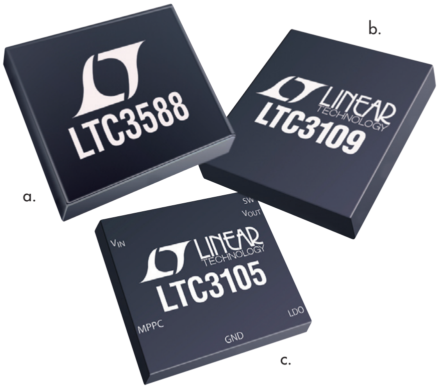
(due to heat) given off by electric motors and can convert this energy to drive wireless sensor networks often without a battery. The EnOcean Inc. ESK 300 version 1 868-MHz wireless energy harvesting development kit is designed to demonstrate EnOcean's energy harvesting and ultra-low-power radio technology *(Fig. 4)*. It comes with two electromechanical pushbutton generators for switches and a solar-powered temperature sensor. Transmissions sent by the self-powered sensors are received via USB dongle and visualized via DolphinView Basic PC software.

The pushbutton radio transmitter module enables the implementation of wireless remote controls without batteries. Key applications include wall-mounted flat rocker switches with one or two rockers, as well as handheld remote controls with up to four single pushbuttons. Designed for linear motion, the kit's ECO 200 energy converter can be used to power the PTM 330 radio module. The energy output at every actuation is sufficient to transmit three transmissions with a free field range of 300 m. Miniaturized switches and sensors in building technology and industrial automation are among the possible applications.

The EnOcean Alliance has created an ecosystem around low-power energy harvesting wireless technology to establish it as a worldwide standard for sustainable building and industrial automation. It will enable the interoperability of different end products based on the ISO/IEC 14543-310 standard.

Low-voltage booster modules are available to amplify low energy harvesting levels for possible battery-less operation like the EH4205 from Advanced Linear Devices. This self-starting module harnesses energy from 70-mV to 4-V sources and draws input power as low as 230 µW, enabling energy harvesting from electromagnetic coils and TEGs.

The EH4205 has a nominal input impedance of 50 Ω, a power efficiency of 52%, and an operating-temperature range of 0°C to 70°C. It inputs energy to dc or ac voltages. Its hibernating function puts it in a zero-power state until the input of the connected energy source becomes active, causing it to wake up, accumulate energy, and function as long as the source is active.

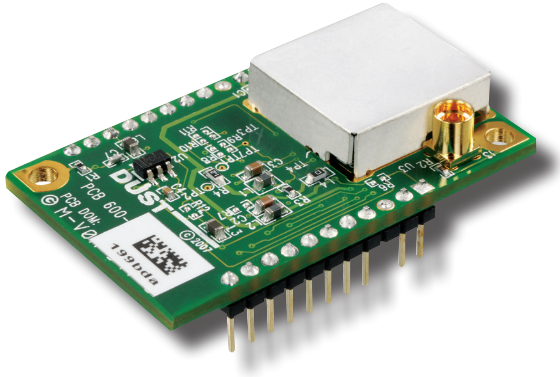


5. Linear Technology supplies a wide range of ultra-low-power modules targeted for energy harvesting applications from piezoelectric and photovoltaic sources as well as thermoelectric generators (TEGs). They include the LTC3588-1/2 piezoelectric energy power supply (a), the LTC3108/9 TEG (b), and the LTC3105 solar energy 400-mA step-up dc-dc converter (c). *(courtesy of Linear Technology Corp.)*

Typical commercially available low-voltage booster modules require at least about 300 mV of input drive to operate. While some off-the-shelf low-voltage modules are available that can operate from about 100 mV, they cannot satisfy energy harvesting sensing applications from such sources as TEGs and photovoltaic elements, which typically output power in the single-digit and double-digit range of some 4 to 40 µW.

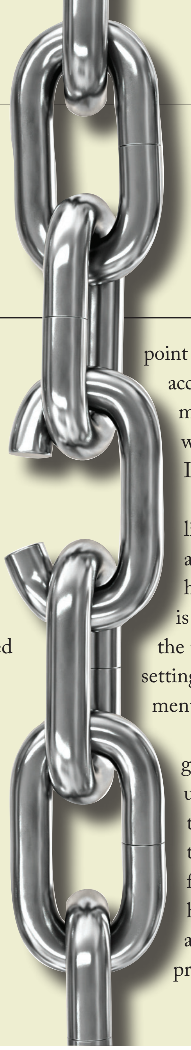
Linear Technology supplies a wide range of ultra-low-power modules for energy harvesting applications from piezoelectric and photovoltaic sources as well as TEGs. They include the LTC3588-1/2 piezoelectric energy power supply, the LTC3108/9 TEG, and the LTC3105 solar energy 400-mA step-up dc-dc converter with maximum power-point control and a 250-mV startup *(Fig. 5)*.

The Dust Networks Eterna transceiver chips implement IEEE 802.15.4e, which came out this year. Together with systems-on-chips (SoCs), this second-generation product features power dissipation levels 50% less than the earlier generation they replace, cementing the company's lead in indus-



6. Dust Networks' second-generation Eterna transceiver chip features power dissipation levels 50% less than previous units. Eterna technology chips consume an eighth of the power of competitive offerings and can last eight times longer. *(courtesy of Dust Networks)*

HOW SAFE IS WIRELESS SENSOR NETWORKING?



ADVANCED HUMAN-MACHINE INTERFACE (HMI) devices like smart phones and tablets may make industrial wireless networking control easier and simpler. But there are risks involved in cyber attacks, some intentional and many unintentional, that can render a plant's operation all but dead unless sufficient safeguards are taken.

From February through April of this year, personnel from cyber security firm Cyberti Corp. covered nearly 4000 miles of roads hunting for IEEE802.11 a/b/g/n wireless transmissions, specifically looking for the organizationally unique identifiers (OUIs) of power control system providers. These OUIs are applied by the network device provider, the vendor of the control system hardware.

Cyeberti's study showed that OUIs and the full media-access control (MAC) address often are left unprotected even in the most secure security settings. Cyberti cofounder and chief security officer Matthew E. Luallen warns that control system protocols like Modbus, EtherNet/IP, PCCC, DNP3, and ICCP are natively unauthenticated, leaving hackers free to do whatever they want, should the data associates control system MAC addresses on an unprotected or poorly protected wireless network. Luallen adds that portable devices may serve as the entry point to the protected control infrastructure using cached remote access credentials and applications stored on them. Wireless devices may also be configured to multihome between IEEE 802.11 wireless networks and cellular networks, creating an unwanted Internet gateway.

"Portable electronic devices must not be categorized as tools like a hammer or wrench. These devices retain information about the control system environment and can cause additional harm if placed in untrustworthy hands. Whether the device is a traditional laptop, iPhone, iPad, or HART communicator, the tool may contain communication points, tags, configuration settings, logic, diagrams, blueprints, and specifics about the environment that a skilled attacker can leverage," Luallen says.

"First and foremost, one must investigate the true productivity gains and reduced costs of using mobile applications that have unfettered access to a control system," he adds. Luallen also says that control system remote access should not be allowed from traditional consumer phones or tablets. "If you have a realistic fear of the cyber risks that exist, you should think long and hard before doing anything that increases your attack surface as much as adding mobile applications can. The risk may well prove to be greater than the actual productivity gained." ■

trial wireless sensor networking *(Fig. 6)*. Dust Networks claims that products based on its Eterna technology consume an eighth of the power of competitive offerings, which means they can last eight times longer and can be eight times "greener" even if they're line-powered.

Not all wireless network transceiver chips are designed to operate over a long range and externally to a plant. Many are designed for short-distance communications and can be used in the industrial space within plants and manufacturing facilities to allow communications between factory floor equipment.

Many of these transceivers are compact, ultra-low-power consuming devices. They also use the Wi-Fi (IEEE 802.11) and ZigBee (IEEE 802.15.4) communications protocols and can operate in the unlicensed 2.4-GHz industrial, scientific, and medical (ISM) band. Others also use the Bluetooth protocol (IEEE802.15.1).

These chips include the SX1231J from Semtech, the ZiC2410 from California Eastern Labs, the Si446x EasyRadioPro from Silicon Labs, the ADF7023-J from Analog Devices, and the C2500 from Texas Instruments.

The Si446x "takes sub-gigahertz wireless technology to a new levels of narrow-band performance and power efficiency," says Silicon Labs' vice president and general manager Mark Thompson. The chip dissipates just 50 nA in sleep mode, making it ideal for energy harvesting battery-powered wireless sensor networking.

One of the most recent transceivers, the self-contained Banner Engineering SureCros Q45 wireless standard photoelectric sensor solution, is designed for control and monitoring applications *(Fig. 7)*. Its proprietary power-management circuit delivers extended battery life up to five years on two replaceable AA lithium batteries, depending on the sensor and application used.

7. This self-contained SureCros Q45 photoelectric-sensor transceiver from Banner Engineering satisfies industrial low-power wireless sensor network applications. Its power-management circuit delivers an extended battery lifetime up to five years for two AA lithium batteries *(courtesy of Banner Engineering Inc.)*