LOU FRENZEL | Communications Editor
lou.frenzel@penton.com

Most industrial monitoring and control functions require networks and I/O interfaces to function.

CONNE

PROVIDES THE LIFELINE OF INDUSTRIAL CONTROL

Industrial control broadly defines the range of electronic equipment used in factories, process control plants, and automated facilities to monitor and control manufacturing and other operations. It involves robots, computers, machine tools, programmable logic controllers (PLCs), sensors, relays, valves, motors, and measuring instruments.

Industrial control is also part of mines, oil and gas production, water and waste water treatment, electrical and gas utilities, and other power generation facilities. Airlines, railways, trucking, and metropolitan transportation systems use industrial electronics as well. Yet one dominant theme throughout all industrial control is communications.

Virtually all equipment and devices rely upon electrical interfaces and networks to function. Over the years, the use of communications equipment has increased and its nature has changed as new technologies have emerged to improve the communications function as well as optimize monitoring and control operations.

TRENDS AND ISSUES

The industrial field generally lags behind other sectors of electronics simply because its technological needs do not follow the consumer or enterprise market trends. But overall, industrial sectors do follow the general trends in communications technology. Key trends and issues include:

- Continued use of fieldbuses: The fieldbuses are the digital LANs of industry. They connect the sensors, controllers, and actuators of most factory automation and process control facilities. Despite the ongoing movement to Ethernet connectivity and wireless, there continues to be growth of several percent per year in the fieldbus market.
- Strong movement to Ethernet: Ethernet has been the local-area network (LAN) of choice for enterprise and even consumer networking for decades, and it dominates. Industry was slow to adopt it but has now embraced it completely. Most new industrial networking efforts use some form of Ethernet. Its proven reliability, low cost, and high availability have made it particularly popular. Special industrial versions of Ethernet have emerged to enhance it for industrial use.
- Significant growth in wireless connectivity: Industry was slow to adopt wireless despite its many benefits. Industrial users assumed it was unreliable and insecure but have learned otherwise since. New and improved wireless standards and equipment have made wireless a key component in most modern industrial settings.
- Fewer proprietary standards and equipment: For decades, industrial communications needs were met with many high-cost proprietary fieldbuses, interfaces, and equipment,

which are still entrenched in many systems. However, the trend today is to open standards and Ethernet.

- Rapid adoption of the Internet protocol (IP) model: The goal is to give most industrial equipment an IP address so devices and equipment can communicate over Ethernet and the Internet. With the availability of IPv6, that is now possible.
- More video surveillance: security is critical to many plants and facilities, and video is useful. Video also enables improved monitoring that simple sensors cannot provide.
- The lingering hodgepodge of equipment: Most factories, process control plants, and facilities are a real mixed bag of old and new, analog and digital, and proprietary and open standards. A big issue has been the incompatibility and interoperability of different equipment. How can it all work together seamlessly? New standards, equipment, and software are gradually addressing that problem.

FIELDBUSES

In the past, control systems in factories and plants were analog in nature. They used direct connections from controller to actuator or transducer to controller and were based on a 4- to 20-mA control signal. As systems became more complex and as networking technologies evolved, eventually a change from the analog system to a digital system came about.

Direct digital control (DDC) systems using a single computer to control a large part of the system came first. Distributed control systems (DCSs) where each device had some intelligence replaced DDC. Programmable logic controllers (PLCs) are also a major part of the equipment mix. Fieldbuses were developed to tie all these digital components together.

Fieldbuses are digital networks and protocols that are designed to replace the analog systems. These industrial LANs network all of the computers, controllers, sensors, actuators, and other devices so they can interact with one another. A single network cable replaced the dozens or even hundreds of individual analog cables in the older systems. Protocols allowed operators to easily monitor, control, troubleshoot, diagnose, and manage all devices from a central location.

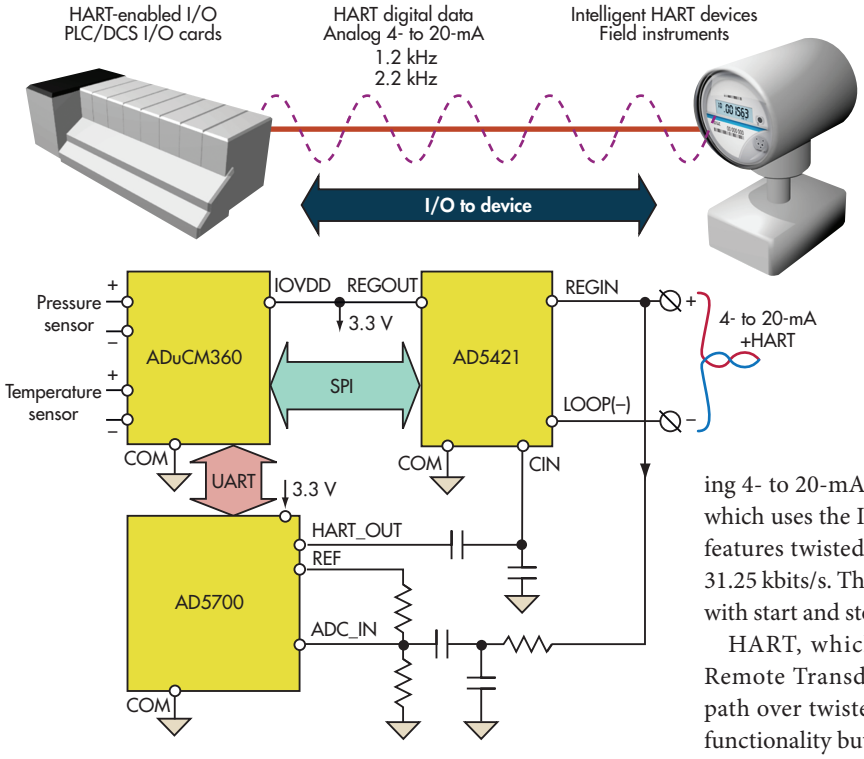
While these fieldbuses reduced the wiring and improved the reliability and flexibility of the system, another issue was created: multiple proprietary systems, with incompatibility and a lack of interoperability between the various components. Devices made to work with one fieldbus and protocol could not work with another.

While some systems could be implemented with a single fieldbus from a single manufacturer, more tended to be "mix and match" systems with components from multiple vendors. The proprietary systems protected the manufacturer's market, but they often created unbearable hardships on the customers and the engineers who had to design, build, and maintain the control systems.

Many fieldbuses have been developed. Some attempts at building a common standard were made but no one system or standard ever emerged. The marketplace weeded out the weaker systems, leaving a few still incompatible standards. ControlNet, DeviceNet, Foundation Fieldbus H1, HART, Modbus, and Profibus PA are the most common fieldbuses.

ControlNet is an industrial network and protocol supported by the Open DeviceNet Vendors Association (ODVA). It is based on the Common Industrial Protocol (CIP), which defines messages and services to be used in manufacturing automation. ControlNet uses RG-6 coax cable with Bayonet Neill-Concelman (BNC) connectors for the physical layer (PHY) and is capable of speeds to 5 Mbits/s using Manchester coding. The topology is a bus with a maximum of 99 drops. Its timing permits a form of determinism in the application.

DeviceNet is another ODVA supported fieldbus. It uses the well-known controller-area network (CAN) technology for the PHY that was originally developed by Bosch for automotive applications. The DeviceNet protocol is similar to that of ControlNet and also uses the Common Industrial Protocol (CIP) at the upper layers. Layers 1 and 2 are CAN bus. The medium is unshielded twisted pair (UTP) using a single-ended non-return-to-zero (NRZ) format with logic levels of 0 V and +5 V. The topology is a bus with up to 64 nodes allowed. Data rate depends on bus length and can be as high as 1 Mbit/s at 25 meters to 125 kbits/s at 500 meters.



1. A HART field bus device can be implemented with sensors, an embedded controller, a DAC, a dc 4- to 20-mA current source, and a HART modem from Analog Devices.

Originally developed by the International Society of Automation (ISA) standards group as Foundation Fieldbus, SP50 was one of the earlier digital fieldbuses for replacing 4- to 20-mA loops. The protocol is designated H1, which uses the IEC 61158-2 standard for the PHY and features twisted-pair cabling with a basic data rate of 31.25 kbits/s. The transmission frames are synchronous with start and stop delimiters. Coding is Manchester.

HART, which stands for Highway Addressable Remote Transducer, is a two-way communications path over twisted pair. It retains 4- to 20-mA analog functionality but adds digital signals. The digital signal is a frequency shift keying (FSK) modulated carrier that uses the old Bell 202 modem frequencies of 2200 Hz for a 0 and 1200 Hz for a 1.

2. The B&B Electronics APXG-Q5420 is an 802.11b/g wireless router and access point. It features one 10/00 Ethernet port and two DB9M RS-232/422/485 ports for serial connected industrial devices.

The data rate is 1200 bits/s. The FSK signal is phase continuous and doesn't affect the analog signal level because it's ac. Also, the FSK signal is a 1-mA variation around the dc level. The protocol uses OSI layers 1 through 4 and 7. The digital part of the communications is primarily used for commands, provisioning, and diagnostics.

The HART fieldbus is popular as it is compatible with older 4- to 20-mA equipment while adding the digital networking capability. It is still widely used. Typical HART field instruments such as the Analog Devices ADμCM360 consist of an embedded controller and the I/O for the sensors such as a pressure transducer and real-time data (RTD) temperature sensor *(Fig. 1)*.

The on-board 24-bit sigma-delta analog-to-digital converters (ADCs) digitize the sensor information and then send it to the AD5421, a digital-to-analog converter (DAC) and 4- to 20-mA current source for connection to the cable. Digital information is also sent to the AD5700 HART FSK modem.

Modbus is a popular industrial protocol normally used for communications with PLCs. It is simple and the standard is open, meaning anyone can use it. It works with RS-232 interfaces. The basic format comprises asynchronous characters sent and received with a UART. Modbus can be carried over a variety of PHYs and is often encapsulated in Transmission Control Protocol/IP (TCP/IP) and transmitted over Ethernet. It is also compatible with a wireless link.

Profibus was developed in Germany and is popular worldwide. There are versions for decentralized peripherals (DPs) and process automation (PA). The protocol is synchronous and operates in OSI layers 1, 2, 4, and 7. Using RS-485, bit rates can range from 9.6 kbits/s to 12 Mbits/s. With a bus up to 1900 meters long, the data rate is 31.25 kbits/s.

INDUSTRIAL ETHERNET

Ethernet has been the LAN of choice for business and enterprise for decades. It is by far the most successful and widely used networking technology in the world. It is affordable and reliable and is backed up by a strong series of IEEE 802.3 standards that keep it current. Over the past 10 years or so, Ethernet has found its way into the industrial setting for I/O and networking. It is gradually replacing the multiple fieldbuses and proprietary networks or working with them. Some of the benefits of moving to Ethernet are:

- Fewer smaller networks: Most fieldbuses can connect up to 20 to 40 devices. Beyond that, a separate fieldbus network is required for more devices and to connect the two networks, if that's even possible. With Ethernet, you can connect up to 1000 devices on the same network. This improves the efficiency and decreases the complexity of the network.
- Lower cost: With many Ethernet vendors, equipment prices are competitive and the overall cost of building a network is typically lower than building a fieldbus network.
- Higher speeds: Ethernet has much higher speed capability than most fieldbuses. While that speed isn't always needed, it is a benefit and the network grows in size and as faster devices are connected. While 10/100-Mbits Ethernet is the most common, some industrial facilities have already upgraded to 1-Gbit/s Ethernet.
- Connection to the factory or plant IT network: The industrial networks are traditionally kept separate from the business network, but companies are finding that advantages occur when the two networks can be interconnected. Data can be collected and used to optimize the manufacturing process or make improvements or decisions not previously possible.

3. Honeywell's Limitless wireless industrial products use the robust 802.15.4 wireless standard. On the far left is the WGLA mechanical limit switch. The unit second from the left is the Honeywell WDRR, a receiver for wireless limit switches that provides inputs for PLCs. The third from the left is the WPMM panel mount monitor unit, which provides LED visual or audio indication for remote limit switch actions. The far right device is the WLS magnetic proximity limit switch. Honeywell's OneWireless Networking products also comply with the ISA100.11a standard.

- Connection to the Internet: This may not be desirable, but if it is, Ethernet provides a very convenient way to send and receive data over an Internet connection.

There are two main downsides of using Ethernet in the industrial setting. First, the hardware wasn't designed for the demanding environment in factories and process plants. Excessive temperatures, environmental hazards, chemicals, dust, mechanical stresses, and moisture make traditional equipment less reliable. Yet over the years, manufacturers have repackaged Ethernet gear to bear up under such conditions by adding industrial-grade housings and tougher electronics.

Another hazard is excessive noise caused by motors, power switching, and other sources. Ethernet's differential wiring is essentially noise resistant. It can be made noise-free with shielded cable. Most industrial wiring is simply standard, but higher-grade CAT5 or CAT6 cable usually suffices.

On the other hand, the RJ-45 connectors are a source of problems, especially in dirty and high-moisture environments. Special RJ-45 connectors have been developed to solve this problem. These connectors add a dirt- and moisture-sealed cover to an upgraded RJ-45 connector. These connectors meet the rigid IP67 environmental standards for hazardous environments.

A second disadvantage is Ethernet's inherent non-deterministic nature. Many industrial networks rely on timing conditions that must occur within a specific time frame. Many need a real-time connection or something close to it. Determinism means a device or system can respond within a mini-

THE INDUSTRIAL CONTROL MODEL

INDUSTRIAL CONTROL APPLICATIONS involve a monitoring function, a control function, or both. Some physical characteristic like temperature, pressure, light, or position usually is monitored. Some cases involve a measurement, meaning some instrumentation equipment is needed. Otherwise the monitoring results in just a "present" or "not-present" signal.

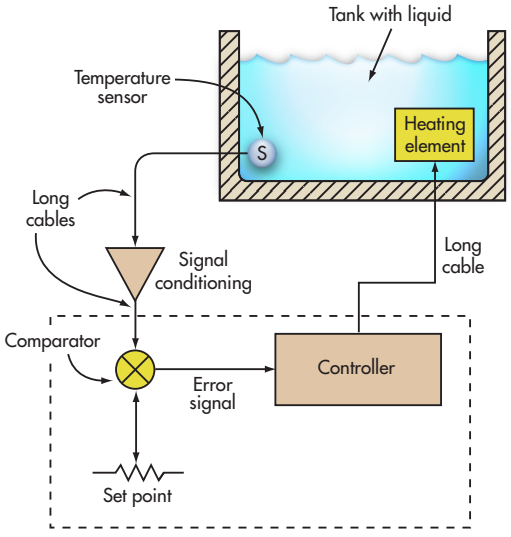
Data acquisition is an example of monitoring where multiple physical characteristics are detected or measured. This data is collected, stored, processed, and ultimately displayed. Data acquisition may not be involved in control operations, where the measured or monitored parameter becomes a feedback signal to effect them.

In control applications, some physical characteristic is changed. Devices like motors or valves are turned off or on or some other physical variable is modified. The state may be either off or on or may be a proportional variation such as speed. Many applications use a combination or monitoring and control operations, which can be classified as either open loop or closed loop control.

Open loop operations normally involve human monitoring and control. For instance, an operator may visually observe the temperature of the liquid in a tank. If the temperature drops below a certain minimum value, the operator manually turns on a heating element to increase the temperature to the desired value.

Closed loop control automates the temperature condition. A temperature sensor sends a signal to a controller that operates the heating element. Therefore, the temperature of the liquid is self-regulating without human intervention (see the figure). The set point is usually a voltage setting that specifies the desired temperature. It is compared to a signal from a temperature sensor that tells the actual temperature.

If the two signals are the same, no action is required.



Most industrial control systems use a closed-loop model. The sensors and actuators often are located at a distance, so some interface or network connectivity is required.

If a difference exists, an error signal is generated, initiating the turn-on of the heating element. As soon as the temperature reaches the desired level, the feedback sensor detects it and the controller shuts off the heating element. This is an example of on-off control. Continuous control would provide continuous power to the heating element and vary the current through it to maintain the temperature more closely.

The various parts of this system are often located remotely from one another. Long cables and interfaces are used to tie all of the system's components together. ■

mum time interval. It can respond in less time but no more than a specified time. If a device is deterministic to 10 ms, anything less is okay. The response does not usually have to be repeatable, but that depends on the application.

Ethernet determinism is widely variable. It is a function of the carrier sense multiple access with collision detection (CSMA/CD) access method, cable lengths, number of nodes, and the combinations of hubs, repeaters, bridges, switches, and routers used in the system. To improve the deterministic response, designers of industrial Ethernet systems must keep cables short and minimize the number of nodes, hubs, and bridges. Switches can be added to larger networks to isolate different segments, and that reduces the number of collisions and interactions.

Determinism can also be implemented or improved in some cases by using the IEEE 1588 Precision Time Protocol (PTP). The PTP permits systems with clocks to achieve synchronization among all connected devices, allowing precise timing information transfer within a network. Time stamping and near real-time performance can occur in some applications.

Another feature of Ethernet finding acceptance is Power over Ethernet (PoE). Defined by IEEE standards 802.3af and 802.3at, it allows the transmission of dc power over the Ethernet cables to power remote devices. This is a major benefit in many industrial settings and eliminates the need to install a power source near some remote sensor or other device. The standard defines power levels up to 15.4 or 25.5 W, but higher-power versions up to 51 W are becoming available.

Finally, several enhanced or modified versions of Ethernet have been developed to overcome the timing issues of standard Ethernet or simply make it more compatible with existing equipment and systems. These include EtherCAT, EtherNet/IP, Profinet, Foundation Fieldbus HSE (high-speed Ethernet), and Modbus/TCP. Some use special protocols while others use TCP/IP.

EtherNet/IP is an application layer protocol using CIP, which defines all devices as objects and specifies the messages, services, and transfer methods. CIP is then encapsulated in a TCP or User Datagram Protocol (UDP) packet for transfer over Ethernet.

Profinet is another protocol that uses TCP/IP over Ethernet. It is not Profibus over Ethernet. Instead, it uses two different protocols: one called Profinet CBA for component-based systems and Profinet IO for real-time I/O operations. Profinet CBA can provide determinism in the 100-ms range. It also can deliver determinism to 10 ms. A version of Profinet IO called IRT for isochronous real-time can have a determinism of less than 1 ms.

Foundation Fieldbus HSE uses the H1 protocol over TCP/IP. It also uses a special scheduler that helps to guarantee messages in known times to ensure determinism at some desired level.

EtherCAT gets rid of the CSMA/CD mechanism and replaces it with a new "telegram" message packet that can be updated on the fly. Networked devices are connected in a ring or a daisy chain format that emulates a ring. As data is passed around the ring, message data can be stripped off or inserted by the addressed node while the data is streaming. The one or more EtherCAT telegrams are transported directly by the Ethernet frame or encapsulated into UDP/IP datagrams. Determinism of 30 μs and less can be achieved with up to 1000 nodes.

Modbus/TCP is the popular Modbus fieldbus protocol packaged in a TCP/IP packet. The Modbus checksum is replaced by TCP/IP's 32-bit checksum. Then the TCP/IP packets are carried over standard Ethernet.

Obviously all of these systems aren't interoperable with one another. But they can all coexist on the same Ethernet LAN since they all conform to the Ethernet Layer 1 PHY standard. Those using TCP/IP could be made interoperable with the appropriate software modifications.

INDUSTRIAL WIRELESS

Wireless technology is a relative newcomer to the industrial scene. Conservative engineers preferred the use of hardwired equipment using cables to ensure reliability in a noisy, interference-prone harsh environment. But wiring is expensive and has other disadvantages. In addition, improved wireless techniques and equipment make it a suitable medium for even critical industrial applications.

Today, wireless is widely accepted as the technology for connecting sensors, actuators, controllers, computers, and data acquisition systems. In fact, modern factories, process control plants, and similar industrial facilities have been covered with multiple networks, including wireless.

Wireless offers significant benefits to industrial connectivity. First, it is time-critical, offering improved response time in some cases over wired solutions. Wireless also eliminates the endless problems with cables and connectors that are common failure points in industrial settings. It is the connection method of choice for hard-to-wire machines, mobile machines, or machines that rotate.

Wireless is especially favorable in applications with long cable runs or where wiring is prohibitive. Such a run could cost tens or even hundreds of thousands of dollars and take weeks to install by a union electrician. Wireless devices can usually be installed and provisioned in minutes. And, wireless devices can be easily monitored or controlled via the Internet and cloud.

One main disadvantage of wireless devices is their need for battery power, since batteries must be frequently changed. This was an initial major knockout factor for wireless sensors and actuators. Changing batteries is a maintenance problem that more plant engineers would rather not face. Today, wireless devices are very power efficient, extending battery life to years. Solar power also is possible in many applications, and other energy harvesting techniques such as vibration are being adopted.

Initial wireless adoption mostly involved proprietary designs for longer distances. Proprietary technologies are still widely used in industrial, scientific, and medical (ISM) band radios for the 902- to 928-MHz and 2.4-GHz bands. However, standard technologies like Wi-Fi and ZigBee are also deployed. And, special wireless technologies have been developed especially for industrial. They feature a mix of noise-mitigating techniques, security, and low latency for highly deterministic applications.

Standard Wi-Fi can be used in some non-critical industrial applications. However, its disadvantages may outweigh the benefits of low-cost, readily available, and easy to install equipment. A host of other wireless gear crowds the Wi-Fi 2.4-GHz band. Interference may too great for a reliable connection in some applications. Latency is long and also a key problem since precise timing is not its main feature. Nevertheless, Wi-Fi is a good fit for some industrial applications *(Fig. 2)*.

Other popular wireless technologies like Bluetooth and Z-Wave also are generally unsuitable for industrial use. Yet one 2.4-GHz technology has emerged as a prime technology for industrial wireless equipment. The IEEE 802.15.4 standard that uses the 2.4-GHz band is especially robust because its frequency-hopping method ensures an interference-free channel and the direct sequence spread spectrum (DSSS) modulation method survives well in a noisy environment.

The standard's 2-MHz chipping provides a processing gain against interference of 9 dB. Its 250-kbit/s basic data rate is fast enough for most industrial uses. A 128-bit AES encryption engine provides security. Its very low duty cycle makes it a very low-power technology. When enhanced, 802.15.4 becomes ideal for many industrial applications. ZigBee, WirelessHART, ISA100.11a, 6LoWPAN, and several other technologies are based on the 802.15.4 standard *(Fig. 3)*.

4. The B&B Electronics Spectre 3G cellular router is a Wi-Fi 802.11b/g/n hot spot but also provides a high-speed link to CDMA or HSPA+ cellular basestations.

ZigBee uses the 802.15.4 standard for the physical and link layers and adds a communications stack that implements mesh networking. Mesh networks are commonly used to form wireless sensor networks that are spread out over a large distance. They extend the range of each sensor and make the connectivity more reliable thanks to the multiple redundant paths possible. Even when nodes fail or noise interrupts one path, another path can be used. Some industrial applications use ZigBee, but other enhanced versions of 802.15.4 are more widely incorporated.

WirelessHART is the radio version of the popular HART field bus. It uses the 802.15.4 standard as its base but adds the upper layers of the system. It provides a time-synchronized, self-organizing, self-healing mesh network based on Linear Technologies' Dust Networks technology. It has always-on security with 128-bit AES encryption and full device authentication.

The basic components are a network manager that sets up and maintains the mesh network, a security manager that handles the encryption keys, a gateway that provides the connection to the host network, a repeater that just routes messages to extend range, an adapter that works with existing HART instruments, and a handheld terminal for routing maintenance and calibration.

The International Society of Automation (ISA) ISA100.11a standard was designed exclusively for the process control industry and general factory automation. The physical and data link layers use the basic 802.15.4 standard. Additional layers of the communications stack implement time division multiple access (TDMA), channel hopping, and mesh-to-mesh routing. This standard also provides a tunneling protocol that permits it to carry existing protocols such as HART, Foundation Fieldbus, Modbus, and Profibus. The frame format complies with the Internet Engineering Task Force (IETF) RFC 4944, an IP-based protocol.

One interesting wireless technology invading the industrial space is 6LoWPAN, which means IPv6 over low-power wireless personal-area networks. This IETF standard is designed to help connect the billions of devices projected for the Internet of Things (IoT) movement. One popular forecast says there will be over 50 billion devices of all sorts connected to the Internet by 2020. This standard will provide some of that connectivity.

IPv6 offers a 128-bit addressing capability, allowing many more IP addresses to be assigned than now possible with the fading IPv4 32-bit capability. 6LoWPAN uses a header compression technique that encapsulates IPv6 packets so they can be carried by 802.15.4 radios. The IETF standard is RFC 4944.

Then there's machine-to-machine (M2M) connectivity *(Fig. 4)*. Known as the Internet of Things (IoT), this movement includes industrial components. M2M applications typically use cellular radios to communicate. These are particularly useful for very remote sensors or other equipment. Low-cost cellular radio modems are widely available for embedding into other units. However, special M2M cellular service with a carrier is required. ed