ZigBee is a wireless networking standard that promises to reshape the way many companies create the infrastructures that their businesses and processes are built on. It will enable reliable, cost-effective, and low-power wireless monitoring and control products based on open standards. This article provides an overview of ZigBee technology and discusses some considerations for use and practical applications, including topologies and cost drivers.

ZigBee has been developed by the ZigBee Alliance, a group of companies working together to create a standard to enable wirelessly networked monitoring and control products based on an open standard.

The primary goals of ZigBee and the ZigBee Alliance are to address the market need for and benefits of standards-based, interoperable wireless products in areas such as industrial process monitoring, home and building automation and control, consumer electronics, medical monitoring, and similar areas. ZigBee is designed to support these goals through simplicity, long battery life, mesh networking capabilities, security, reliability, and low implementation cost.

The ZigBee Alliance provides standards definition, interoperability testing, certification testing, and branding for ZigBee devices to ensure they meet all applicable standards and interoperate as intended.

The building blocks
The ZigBee specifications are designed to accommodate sensing and control networks with a wide variety of devices, a large number of devices (up to 65,000), low active duty cycles, small data packets, and very long (multi-year) battery life.

ZigBee defines a set of higher level protocols built on top of the IEEE 802.15.4 networking standard. It provides network routing and meshing capabilities, security, and support for both standardized and proprietary devices through the use of ZigBee profiles. Designed for use with small processors using battery power, ZigBee enables sensing and control applications that until now were either not practical or even possible.

Using frequency ranges of 868 MHz, 902-928 MHz, and the 2.4 GHz band, ZigBee operates at data rates of 20 Kbit/sec to 250 Kbit/sec depending on the band in use. Ranges of 10-100 meters between devices are obtainable, and when multiple devices are joined into a meshed network, the range can be greatly extended through the relaying (or routing in network terms) of packets from one node to another.

ZigBee networks consist of a mixture of Full Function Devices (FFDs) and Reduced Function Devices (RFDs). In addition to sensing or control capabilities, FFDs can function as network routers allowing them to form a continuous, multi-pathed, and highly reliable network. RFDs are designed to be simpler, less expensive devices focusing on their control or sensing roles. Each RFD communicates to the broader ZigBee network by associating itself with an FFD, which routes data on its behalf.

Security is an important aspect of ZigBee. Wireless networks offer flexibility, but often at the cost of reduced data security. ZigBee supports a variety of security strategies ranging from the IEEE 802.15.4 security for single hop transmissions all the way to Advanced Encryption Standard (AES). The AES standard uses a core encryption algorithm to support confidentiality, integrity, and authenticity of transmitted data across the entire network. With security built into ZigBee right from the onset, ZigBee helps to ensure that data gets to its intended destination and only its intended destination.

Network topologies and capabilities
ZigBee supports several network topologies including star, cluster, and mesh. By supporting these different topologies, a ZigBee network can accommodate many different application, installation, and deployment circumstances.

Among the key attributes of a ZigBee network is the ability to add and remove devices on an ad-hoc basis and the ability to have the network form a mesh of connections between nodes.

Unlike networks designed for more static configurations, ZigBee allows devices to join a network very quickly (typically <30 ms) and supports very quick wake-up and data transmission (typically <15 ms). This permits new devices to rapidly join a network or quickly wake and send data allowing battery-powered nodes to spend most of their time in a very low power sleep state and extend battery life to multiple years.

The ability to form a meshed network allows for multiple paths for data within the network and allows extended coverage far beyond the radio range of a single device. Multiple paths provide redundancy and reliability by automatically dealing with temporary signal blockages, such as a vehicle being parked in a signal path between two nodes, or equipment failures. When signal blockages clear, failed equipment is replaced, or new nodes are added to the network; the network can find these new potential routes automatically and use
Networking: Technology

them to benefit the overall network. When using a mesh topology, the total area of a ZigBee network can be much larger than the range of a single RF signal.

ZigBee supports other network topologies as well. Installations based primarily on a single, well located router can configure themselves as a star network using direct, point-to-point communication. Cluster topologies can support groups of devices while still permitting communication between devices in other clusters as shown in Figure 1.

ZigBee networks are formed around a single initial device, the ZigBee Coordinator. The Coordinator chooses a radio channel for the network and controls the overall network topology by specifying key networks parameters affecting the way network formation will occur.

Routers are responsible for the structure and operation of a ZigBee network. They form the backbone of cluster or mesh networks, support the establishment and maintenance of the routes through the network, and perform the actual routing operations (the handing off of packets to specific neighbors who will then relay the packets until they reach their final destination). In the event of routing failure, routers can discover alternate routes to keep traffic moving and can also discover more optimal routes as the network grows.

ZigBee sensor networks
A typical ZigBee sensing network involves a set of ZigBee-enabled sensors with some number of ZigBee routers and a ZigBee Coordinator (typically a router with Coordinator capabilities). In addition to the actual sensor or controller interfaces, a sensor node requires a ZigBee-capable radio and a small microcontroller as illustrated in Figure 2.

In some cases, a gateway device may be deployed to support connections into and out of the ZigBee network to external networks or devices.

Profiles
Profiles provide a means to identify and locate devices of particular types or that provide particular services. For example, a light switch can locate a light load controller (or vice versa). Beyond simply locating a device, ZigBee applications can determine detailed characteristics of devices or applications that enable a fine degree of control and a high level of useful interaction.

For example, a ZigBee light switch can not only find and associate with a ZigBee lighting controller, it can determine whether or not the controller is capable of dimming its load or whether it supports optional capabilities, such as sensing its current lighting level or whether the room the lighting controller is located in is occupied or not.

ZigBee profiles enable devices to find and effectively communicate with other network devices using standardized requests, and operations. The support of profiles is the cornerstone of ZigBee interoperability.

Using ZigBee effectively
Deploying successful ZigBee networks requires some understanding of the type of communications needed, the power requirements of the devices, ranges and densities of the radio devices, and the costs of deployment and maintenance.

ZigBee application characteristics
ZigBee is focused on applications with particular characteristics. ZigBee is best suited for applications requiring periodic or intermittent data of relatively modest size. Typically, this is 40 bytes or so of data. While this is a relatively small, it is usually more than enough for most sensing and control applications. Sensed conditions like temperatures or pressures can typically be expressed in 1-4 bytes and control directives are often similarly sized.

Since many ZigBee sensors are intended to be battery-powered, the use of compatible sensing and control technology is crucial. In these situations, sensors must be “battery friendly.” This includes operating on available battery voltages without excessive current draws that would impact battery life. Additionally, sensors should support a low power consumption mode or even completely shut down to save power when the battery-powered node goes to sleep. Sensors should be able to wake quickly without excessive power consumption or long delays that would impact battery life. Controller applications are subject to similar considerations.
One way to work around battery limitations is to leverage existing power from the machine or device being monitored. Many machines have internal power sources, which can power wireless sensing nodes with minimal impact. The low power requirement of the typical ZigBee node provides flexibility in regard to input voltage and current, which can ease the integration into existing systems and devices.

**Radio range and density**

With ranges of 10-100 meters, radio placement must be taken into account when deploying ZigBee devices in order to create an effective and reliable network. By locating battery-powered sensors and mains-powered routers in a way that multiple devices are within RF range, an effective mesh can be created offering more routes, higher reliability, and redundancy.

Due to the ad hoc nature of ZigBee networks, additional routers can be easily added to an existing network without shutting down or restarting to provide new network paths quickly and easily. A few strategically positioned routers can greatly improve the network infrastructure of a ZigBee network and can be easily added at any time.

**Costs for wired vs. wireless sensor networks**

In many locations, typical costs for the professional installation for a wired device including material (such as wire, conduit, and fittings) and labor can be $10 per linear foot or higher, with most of that cost in labor. If a $20 sensor requires 100 feet of wiring to install, the effective cost of deploying that sensor may be $1,020. Conditions such as wet or explosive environments require special wiring components and installation expertise that can dramatically increase costs.

While a ZigBee network may save wiring costs, there is a cost for the radio, processor, and other components necessary to wirelessly enable a device. The cost for an 802.15.4 radio transceiver, 8-bit microcontroller, support components, battery, and ZigBee software can be less than $25 per device in small quantities.

When evaluating ZigBee as a potential replacement for wired networks, it’s important to account not only for the cost of the individual components but the total deployed cost. In the previous example, the cost of the sensor is more than doubled when ZigBee-related components are added, but when compared with the total cost of a wired installation, a ZigBee solution is actually a fraction of the installed cost.

Any sensing or control network consists of more than just the individual sensing and control nodes and must include network infrastructure such as control panels, logic controllers, and other network support devices. ZigBee networks require a Coordinator and routers in addition to the sensing and control nodes. Depending on the size and configuration of the network, additional routers may be needed to extend the reach of the network to all devices. While these infrastructure costs cannot be eliminated, the incremental cost of adding nodes to a ZigBee network is only a fraction of the cost of adding nodes to a wired network.

Installation costs are not the only expenses, so it is important to consider the total life cycle costs for the network. As an example, wired networks often require physical reconfiguration, which can be a substantial cost, and networks of battery-powered sensors will require periodic battery replacement. Evaluating technologies on both deployment and ongoing maintenance costs can help present a clearer picture of the overall cost of a potential solution.

**Practical ZigBee applications**

Practical ZigBee applications are those where there is a clear way to realize a return on the investment of wirelessly enabling sensor or control networks, either through direct cost savings or by enabling solutions that were cost-prohibitive without this technology. Oftentimes, this comes from exploiting the unique capabilities of ZigBee networks, such as low power requirements or support for ad hoc network changes.

Using the battery-powered capabilities of ZigBee networks can simplify dealing with explosive environments, such as the production of ethanol or other fuels. With a wireless connection between a sensor and its control logic, expensive and difficult-to-install explosive-safe connectors, housings, and bulkheads are eliminated. In addition, battery-powered sensors operating on less than 5V are intrinsically explosive-safe, saving hundreds of dollars in special sensing nodes and installation costs (many ZigBee radios and processor combinations can operate)

The ad-hoc capability of ZigBee can be used for cost-effective monitoring of a fleet of commercial vehicles. By supporting ZigBee devices integrated with a vehicle’s on board diagnostic or sensing capabilities (such as ODB-II), a plethora of information can be collected when a vehicle returns to the maintenance or rental facility. This data can identify vehicles with specific problems or vehicles whose loads or mileages indicate regular maintenance is warranted. The rapid network joining and ad-hoc networking capabilities of ZigBee support collecting information quickly from vehicles as they enter a facility with no manual intervention or configuration.

For more information

The ZigBee Alliance website, www.zigbee.org, provides information regarding the ZigBee networks, the ZigBee protocol, and suppliers of ZigBee-compatible components, systems, software, and engineering services.

For more information on the IEEE 802.15.4 networking standard, see the IEEE 802.15.4 website at www.ieee802.org/15/pub/TG4.html.

**Chris Herzog** is the President of Software Technologies Group, a software engineering services firm with a focus on 802.15.4 and ZigBee technologies, including software protocol stacks, development tools, prototypes, and product development.

To learn more, contact Chris at:

Software Technologies Group
10300 W. Roosevelt Road, Suite 310
Westchester, IL 60154
Tel: 708-547-0110
E-mail: c.herzog@stg.com
Website: www.stg.com
Networking: Technology

Deploying ZigBee in existing industrial automation networks

By Tim Cutler

ZigBee technology has industrial networks as one of its primary targets. Implementation of ZigBee-enabled devices is attractive, but in many cases coexistence with existing networks is required. This article looks at ways to incorporate ZigBee-enabled devices into existing network topologies effectively, gaining the benefits while preserving existing investments.

The ZigBee wireless standard is gaining favor fast in industrial arenas, where it is prized for its low cost and its mesh networking capabilities. The immediate challenge to realizing ZigBee’s many benefits, as with all new technologies, is implementation without extensive re-engineering.

For many early adopters, the answer will come with gateway and sensor modem techniques that marry ZigBee with existing system components. Products incorporating these techniques are already entering the market, providing immediate over-the-air mesh links between existing PLCs and remote devices, and preserving the usefulness of existing monitoring programs, even as they lay the groundwork for embedded ZigBee systems of the future.

The foundation of automation networks: PLCs, sensors, actuators

Regardless of specific application needs, industrial automation networks consist of PLCs (programmable logic controllers) that communicate with remote sensors to gather data regarding such variables as pressure, temperature, vibration, sound, and strain. When the application includes a control function, PLCs act on that data by issuing commands that orchestrate processes among such actuators as relays, motors, solenoids, and valves. An example is shown in Figure 1.

The success of this automation depends on reliable communications between PLCs and sensors/actuators. The communication links have traditionally been hard-wired, with data transmitted over cable.

In most cases, communications is driven by the openly published Modbus protocol, supported by the majority of PLCs, sensors, and actuators used worldwide. The ubiquity of Modbus and the sensors and actuators that support it represent enormous investment, and an entrenchment that makes inroads difficult for alternative technologies.

The basic need for wireless

Despite its advantages, wired industrial networking has well-known drawbacks. Data cabling represents a tremendous labor cost, in both initial runs and in reconfiguration.

The cables themselves are unwelcome in many factory environments, where they can represent nuisances or safety hazards. And cabling runs have severe length limits, leaving networks unable to address very remote sensors and actuators in such environments as oil fields and large-scale plants.

Wireless networking has always been a reaction to these issues, with a primary requirement of preserving communications reliability. Because factory and industrial settings pose special challenges for wireless transmission, most notably in interference and multipath fading, industrial wireless solutions employ special techniques to compensate for noise and interference. One successful method has been Frequency Hopping Spread Spectrum (FHSS), which ensures reliable data delivery in point-to-point and star topologies. Another is mesh networking, which uses automatic routing techniques to redirect transmissions that fail in any transmission path.

While these solutions are effective, they are generally found in pockets of need rather than serving as entire network platforms. One reason for this is the proprietary nature of available solutions. Unlike Modbus in the wired arena, the industrial wireless market has been characterized by proprietary solutions that don’t interoperable with products from competing companies (the 802.11b and Bluetooth standards were created for very different applications, and have limited use in industrial settings). Another reason is cost, with solutions of any technology typically costing upwards of $100 per node, sometimes much more.

For these reasons, wireless remains an alternative, rather than mainstream, transport mechanism, flourishing...