

Bluetooth technology has been highly touted in the media as the next wave of connectivity promising an end to the clutter of wires, and facilitating mobile synchronization of data in the era of hybrid PDA/cellular phones.

Over 2,000 companies have already signed up with the consortium, hence each of the last three years has been heralded as the one in which Bluetooth “explodes onto the market.”

Many manufacturers will be surprised to learn that even though Bluetooth was introduced in 1994, it has not yet gained traction. A quick market review indicates that the standard is still a concept more than a reality.

Here’s a look at some common misconceptions surrounding Bluetooth and its deployment...



You  
should  
integrate  
**Bluetooth**  
for its  
low cost &  
universal  
acceptance.

“Bluetooth” is the name given to a communication standard whose focus is ubiquitous, low-cost, short-range wireless connectivity between diverse devices—principally cellular phones, headsets, laptop PCs, automotive telematics and PDAs.

The Bluetooth specification defines a short- to medium-range radio link capable of voice or data transmission up to 720Kbs per channel.

Radio operation is in the unlicensed 2.4GHz ISM band, using a spread spectrum, frequency hopping, full duplex signal at up to 1600 hops per second. The signal hops among 79 frequencies at 1MHz intervals to provide interference immunity.

RF output is specified as 0dBm (1mW) in the short-range (10m) version and 20dBm (100mW) in the longer-range (100m) version.

**You Need AeroComm.**

**Wireless Myth #4**

**Fact:**

## “Bluetooth will be ubiquitous.”

Universal acceptance is achieved when products perform better than alternatives at an acceptable cost, and the benefits extend to the layman user, not just to the techie. To become ubiquitous, Bluetooth must first be embedded into backbone devices such as laptops, phones and PDAs. These devices must be easy to design, set up and operate, and then interoperate seamlessly. Plus, the cost of adding Bluetooth to the device must not exceed its benefits.

None of these factors are true today.

## “Bluetooth costs \$5.”

The genesis of this myth is not known, but the concept is driven by market need, not technological reality. Bluetooth chipsets in 1M volumes may cost \$5; however, a chipset is not a radio. Recent costs for modular Bluetooth short-range radios were \$25 to \$30 in 10K volumes. There are additional costs for antennas and processors to control the radios.

At the early stage of roll out of Bluetooth technology, the OEM will often supply both ends of the RF link until Bluetooth is available in backbone devices. Assuming normal OEM cost-to-consumer-price ratios (4:1), Bluetooth adds \$100 to \$120 per node, clearly too high to become ubiquitous.

## “Either 802.11-compliant or Bluetooth radios will win the market, so I must choose one.”

OEMs should actually consider their applications and choose appropriate RF solutions. Most experienced observers predict that the market will group as follows:

**802.11 or WLAN** will likely dominate the PC networking market, principally connecting notebooks to corporate networks or similar settings where cables are inconvenient, such as inside homes.

**Industrial RS232 RF modules** will capture industrial segments that require robust performance and prefer to segregate communication within the network.

**Bluetooth** will likely perform best as a cable-replacement system in consumer applications, particularly with companies that can allocate the extensive development resources required.

## “It’s safest to go with an industry standard.”

It is much too early to tell if Bluetooth will ever establish itself as a widespread standard. The OEM must weigh the benefits of the standard against the additional burdens it places, such as standards compatibility, significant extra software development, and interaction with devices and radios not yet conceived.

## “Bluetooth technology is easy enough for non-RF OEMs to integrate.”

To operate in such a noisy band, Bluetooth requires a very robust approach regarding interference and security. This includes protection measures such as encryption, pairing, and authentication of devices, as well as frequency-hopping schemes. The complexity will generally restrict Bluetooth to those OEMs with significant RF expertise, superior protocol development, and high-volume production to support the overhead.

## “Simply buying a Bluetooth chipset and placing it on my board will make a nice RF link.”

Integrating a radio is much more complex than adding other peripheral devices. First, a radio faces unique physical challenges that often change and may be difficult to control. Two principal examples are antenna selection/placement and protocol development.

**In terms of antennas**, Bluetooth radios output very low power; hence antenna performance is critical. The designer must have a strong knowledge of antenna styles, propagation patterns, mechanical engineering, cost efficiency and industrial design. The antenna must perform well in the intended application with numerous sources of interference, attenuators such as the human body or the system itself. Expensive equipment is required to measure and tune antennas. Once the proper antenna is chosen, each product must be agency-approved with the chosen antenna.

**For protocol development**, the OEM must have access to engineers with RF expertise. Consider this scenario to illustrate the point: small groups of radios form a piconet. In our example, a woman is communicating from her cell phone to a cordless headset using

Bluetooth. To achieve the performance required for streaming audio, the two radios consume the bandwidth for the piconet. When an associate walks into the room with another Bluetooth-enabled phone, that radio emits beacons alerting others to its presence. The woman’s two devices must have protocol to either allow the radio into the piconet or exclude it. If allowed to enter, some bandwidth must be allocated to the third device. If the piconet excludes the third radio, the piconet must deal with the repeated beaconing interference.

Bluetooth operates as a master/slave architecture. A single radio assumes the role of master. Should the master be turned off or leave the piconet, the OEM protocol developers must write software to determine who and how the network assigns another master.

## “Bluetooth’s specification/testing process assures that my system will operate with all other radios.”

Bluetooth’s Qualification Program ensures global interoperability between devices regardless of the vendor and the country in which they are used. During the test procedure that all devices must pass, they must be verified to meet requirements regarding radio link quality, lower-layer protocols, profiles, and info to end users.

The OEM must allocate engineering resources to determine appropriate compliance profiles, develop the system, and submit products to compliance testing—a lengthy and costly process.

## “Because I’m using reputable chipsets, passing FCC, IC, ETSI and SAR tests should be a breeze.”

An OEM has two source alternatives: choose a complete RF module or design one using chipsets.

**Modular solutions** should be pre-approved if you choose antennas from their approved lists. But if your application requires different antennas, subsequent lab scans and agency submissions will be required

**Chipset solutions** require agency approvals. Many devices used in portable or mobile applications require SAR (Specific Absorption) tests to assure safe use close to the body. Agency approvals require in-house equipment and expertise in addition to time-consuming and expensive lab testing.

## “If I buy a Bluetooth module or follow the application notes, Bluetooth certification is assured.”

The principal reason Bluetooth has lagged to market is that its complex protocol exceeds the capabilities of most OEMs. Each RF integration is unique. The OEM must test the device in the field with unanticipated interferers, with obstacles, and with competing Bluetooth devices to assure performance.

## “I can purchase a Bluetooth protocol stack if I don’t want to develop it internally.”

Some licensable protocol stacks will assist the OEM integrating Bluetooth. These typically cost \$50,000 to \$100,000. While these stacks address common issues such as acknowledgements and retries for reliability, the OEM will inevitably have unique needs that will require some custom development.

## “If I need longer range, I can just substitute a higher-power Bluetooth radio.”

Bluetooth is arranged into piconets (small groups of radios within 10 meters of each other) and scatternets (groups of piconets). By increasing the power output, you can dramatically widen the area of impact.

However, the protocol must be developed to handle interference from many sources. For example, the sales department’s piconet can “hear” radios used in the R&D department, manufacturing, etc. Do you let them into the net and allocate a time slot, or do you exclude them and deal with the interference?

## “Bluetooth must have reliable security provisions to guard against eavesdropping by other devices.”

Bluetooth – as with 802.11 – allows any compatible device to listen in. Hence the OEM must **implement** and the user must **enable** encryption. Numerous reports have revealed deficiencies in WEP security with 802.11. Most OEMs would be advised not to use Bluetooth for applications that require tight security, such as financial transactions.