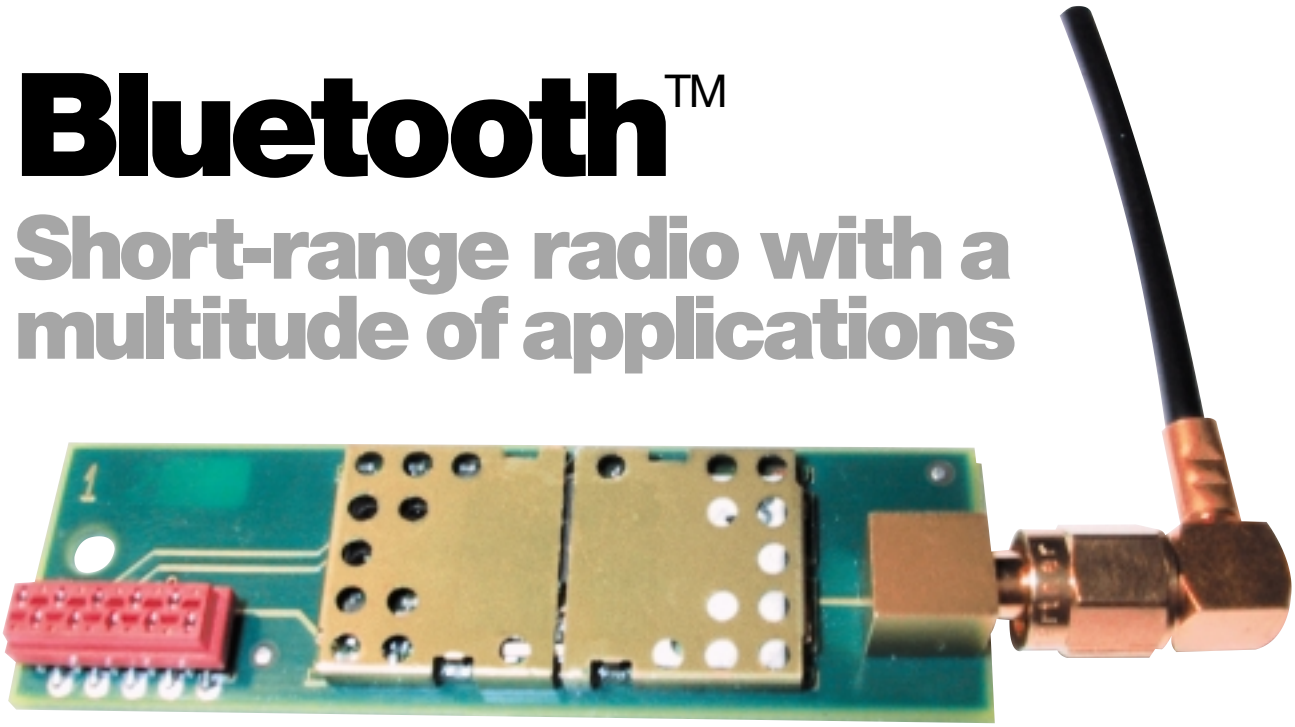
Bluetooth™

Short-range radio with a multitude of applications



Jan Endresen, Torkil Brunsvik, Håkon Beckman, Snorre Kjesbu

Who can honestly say that he or she hasn't at some time looked at the tangle of cables behind the hi-fi or PC without wondering if, in a more perfect world, it couldn't be replaced by wireless connections?

This sentiment is echoed throughout industry. If you think your hi-fi cabling poses a problem, then spare a thought for the unfortunate maintenance engineer as he approaches a defective production machine – and the daunting prospect of having to sort through hundreds or even thousands of sensor wires, data and control cabling, and power feeds.

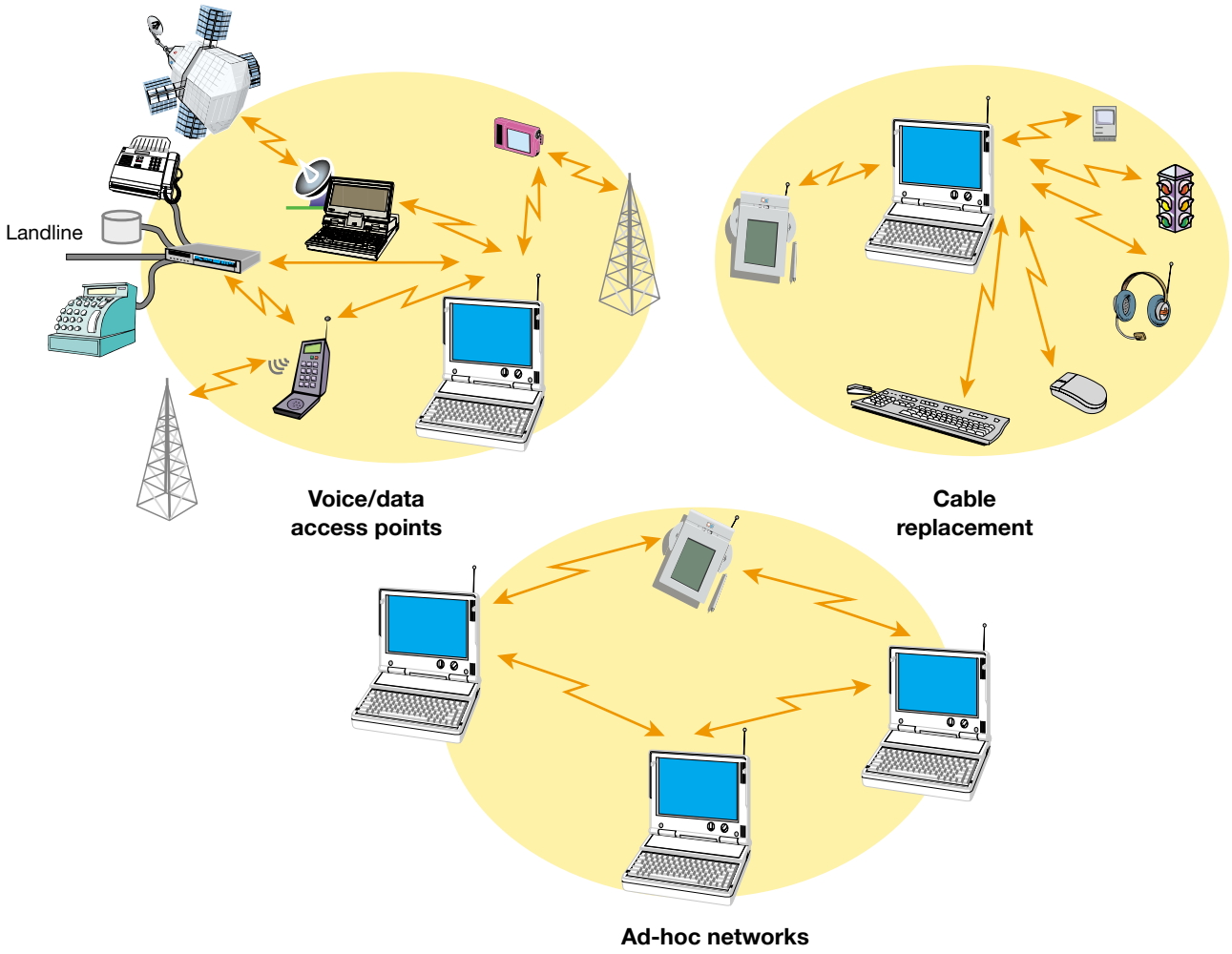
Help is now at hand. A new, short-range wireless link open standard called Bluetooth™ – easy to connect and working in a license-free radio band – is set to revolutionize the way industry communicates with and within itself. ABB is among more than 2000 companies worldwide who have eagerly 'adopted' Bluetooth. Tests carried out to date point to a promising future for the new standard.

To describe what Bluetooth can be used for is like looking into a crystal ball and predicting what will happen in the future. The only thing of which we can be certain is that it will have many, as yet still unimagined, applications.

The first major application of Bluetooth will be in 'mobiles'. The term 'mobile' covers a lot more than just the mobile, or cell, phone, as it will include such things as portable PCs, Wireless Application Protocol (WAP) phones, Personal Digital Assistants (PDAs) and so on. This will allow you to have a wireless headset which can also be connected to your Walkman or MP3 player. The mobile could be connected to your camera (video or still) for transferring your snapshots, or it could be used for a video conference. And in airports you will no longer have to search for the information board – all the flight arrival and departure information will be available on your mobile.

Just as importantly, Bluetooth will enable you to get rid of most of those

1 Potential Bluetooth™ applications are everywhere.



Bluetooth™ – All for one, and one for all

Bluetooth is a communication standard for short-range radio links that promises to rid industry and our homes of the unmanageable mass of cables interconnecting machines and appliances. Issue 1.0 of the Bluetooth specification was released in July 1999 [1] and has already gained wide acceptance due to its low cost and the fact that it is an open standard operating in a license-free frequency band.

A Special Interest Group (SIG) formed in February 1998 to develop and promote the Bluetooth standard for local *'ad hoc'* connectivity between devices from different manufacturers is now more than 2000 strong, and includes ABB among its members. SIG's founding members included Ericsson, IBM, Intel, Nokia and Toshiba. They were joined in late 1999 by 3COM, Lucent, Microsoft and Motorola. There is an ongoing effort to make Bluetooth the basis of the IEEE 802.15 standard, Wireless Personal Area Network (WPAN).

cables connected to your PC. Whether we shall see wireless transfer of power to your keyboard and mouse, or if they will be battery powered, is still an open issue. Your PC will, of course, transfer information to and from your PDA using Bluetooth. The printers will also be equipped with Bluetooth. If you need to print out something from your PDA, you will simply walk up to the printer and do it. There will be no need to first connect to the Local Area Network (LAN) or transfer the information to your PC.

There will be Access Points giving Bluetooth users access to all the traditional networks like the Plain Old Telephone System (POTS), Integrated Services Digital Network (ISDN), Global System for Mobile communication (GSM), Wide Area Network (WAN), etc.

Your car will certainly have Bluetooth devices in it. Every time you drive into a service area, the car will tell you what it needs. As you drive along the highway, local information points will download useful information, like traffic conditions ahead, the nearest hotel vacancy, or information about some scenery worth looking at. Bluetooth may even replace some of the wiring needed for operation and control of the car, thus providing higher functionality and flexibility.

We will have Bluetooth in the home. There will be just one remote controller for everything from the multimedia system to the heating and ventilation systems. Voice, data, music and video can all be transmitted locally using Bluetooth. The various appliances will also be able to communicate. We will be able to control the cooker or turn on the coffee maker, or the fridge will order fresh supplies when the stock is running low or is too old. The cordless telephone could be based on Bluetooth. Further, Bluetooth can provide Internet access from anywhere in the house or nearby.

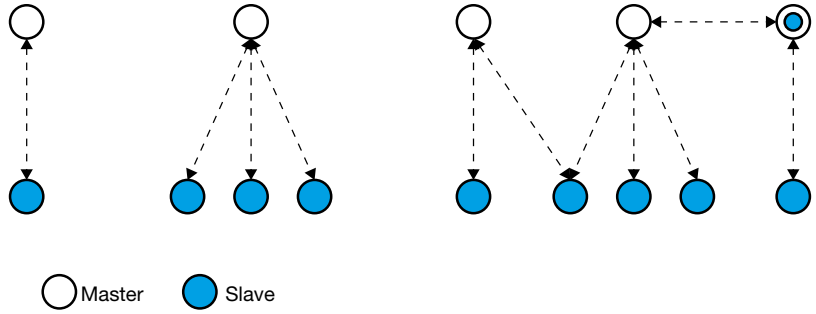
Bluetooth primer

The name Bluetooth comes from the name of the Danish King Harald Bluetooth, born 908, who united Denmark and Norway [2]. The analogy is, perhaps, that Bluetooth will unite computers and telecommunications.

Abbreviations used in this article

ACL	Asynchronous ConnectionLess
ARM	Advanced RISC Machines
ARQ	Automatic Repeat reQuest
ETSI	European Telecommunication Standards Institute
DECT	Digital Enhanced Cordless Telecommunications
FSK	Frequency Shift Keying
GSM	Global System for Mobile communication
HCI	Host Controller Interface
IrDA	Infrared Data Association
ISDN	Integrated Services Digital Network
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
L2CAP	Logical Link Control and Adaptation Protocol
MAC	Medium Access Control
PDA	Personal Digital Assistant
PCM	Pulse Code Modulation
POTS	Plain Old Telephone System
RFCOMM	Radio Frequency COMM
SCO	Synchronous Connection Oriented
TDD	Time-Division Duplex
UART	Universal Asynchronous Receiver Transmitter
USB	Universal Serial Bus
WAN	Wide Area Network
WAP	Wireless Application Protocol
WPAN	Wireless Personal Area Network

2 Different Bluetooth topologies (two Piconets and a Scatternet)



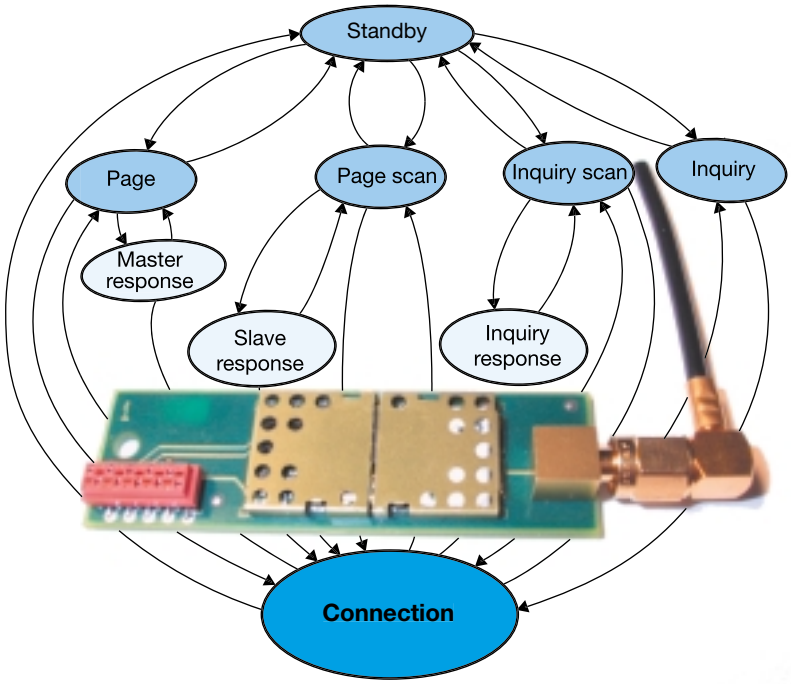
Bluetooth will be used primarily to replace cables by short-range radio-based connections for mobile phones, Personal Digital Assistants (PDA), notebooks, portable or fixed electronic equipment, etc 1. It is also likely to replace infrared links since it depends much less on a direct line-of-sight. Of course, there are alternatives to Bluetooth in certain applications, such as voice and data access points, where Digital Enhanced Cordless Telecommunications (DECT), HomeRF or Wireless-LAN can be used. Moreover, cable could also be replaced by DECT. What makes Bluetooth unique is that it can be used for so many different applications.

Bluetooth radios operate in the Industrial, Scientific and Medical (ISM) frequency band of 2.4 to 2.4835 GHz, which is available globally. Bluetooth uses a pseudorandom frequency hopping spread spectrum technique. It uses 79 1-MHz channels. The nominal hop rate is 1600 hops/s, which is reduced to 320 hops/s if the maximum packet length is used. Bluetooth uses a Time-Division Duplex (TDD) scheme allowing the master and a slave to transmit alternately, which simplifies the radio frequency components. The modulation is Gaussian-shaped binary Frequency Shift Keying (FSK).

The basic topology of Bluetooth is a Piconet, with one Bluetooth module as the master and up to seven other modules as active slaves. The topology can be extended by combining a number of Piconets into a Scatternet, where a slave can be a slave in several Piconets or master in one and a slave in another 2. A Bluetooth module can only be master in one Piconet. The configuration of a network is established in an ad-hoc fashion, allowing new masters or slaves to be added at any time.

Bluetooth provides voice or data services, or both at the same time. The link between the master and a slave can be Synchronous Connection Oriented (SCO) or Asynchronous ConnectionLess (ACL). The SCO is a point-to-point full-duplex link, and is typically used for a

3 Complete Bluetooth module with antenna and external connector



voice connection. A Bluetooth module can support up to three simultaneous voice channels. The ACL supports full-duplex and asymmetric modes (different data rates in each direction of the link). The gross bit rate of a Piconet is 1 Mbit/s, which is shared between the master and the active slaves. If there is only one active slave, the maximum data rate is 432 kbit/s for a symmetric and 721 kbit/s for an asymmetric channel.

A main use of Bluetooth is in battery-powered equipment. To facilitate this, Bluetooth has three low-power modes, called Hold, Sniff and Park, in addition to the standby mode. In the low-power modes, the module needs only to keep a timer running, the rest of the circuitry can be turned off. Returning to the active states takes about 2 ms. In the Park mode the Bluetooth device releases its Medium Access Control (MAC) address, allowing a Piconet to have up to 255 non-active slaves.

Complete Bluetooth modules are available, one being the Ericsson ROK 101 007 3. Currently a hybrid chip, it will be fully integrated in the future, with a price target of USD 5 for large quantities. It contains a complete radio as well as an Advanced RISC Machines (ARM-7) processor which controls the radio and handles the lower layers of the Bluetooth protocol stack. The chip has three hardware communication interfaces, a Universal Asynchronous Receiver Transmitter (UART) for data, Pulse Code Modulation (PCM) for voice, and a Universal Serial Bus (USB) for data and voice.

Bluetooth supports a number of protocol stacks for a variety of applications. The three lower layers, ie the Bluetooth Radio, the Baseband and the Link Manager, are always present. The voice protocol is optional. The Baseband handles the timing, hop selection, packets, error control, etc; the Link Manager handles the link set-up, device authentication and link control. There are two other main protocols specified in Bluetooth, the Logical Link Control and Adaptation Protocol (L2CAP) and Radio Frequency COMM (RFCOMM), which provides an emulation of up to 60 concurrent logical serial ports and utilizes the L2CAP. RFCOMM is a simple transport protocol based on the European Telecommunication Standards Institute (ETSI) standard TS 07.10 with some adaptations. L2CAP provides connection-oriented and connectionless data services with multiplexing capability as well as segmentation, re-assembly and group abstractions.

There is a Host Controller Interface (HCI) defined in the Bluetooth specification which provides a command interface to the Baseband controller and the Link Manager as well as access to the hardware status and control registers 4. This interface fits well with a fully integrated Bluetooth module and in situations where the higher layer protocols are implemented on a separate host processor.

Profiles are specified in Bluetooth [3] for applications such as:

- Dialup networking
- LAN access
- Cordless telephony
- Intercom
- Serial port
- Headset
- Fax

Bluetooth has the normal set of error control mechanisms, such as Forward Error Correction and Automatic Repeat reQuest (ARQ). Together with frequency hopping, they provide a powerful defense against random noise and interference. Security in the form of authentication and encryption is also provided as an option. The four security entities used are summarized in the *Table* (page 40). The Bluetooth device address is the 48-IEEE address, unique to each Bluetooth device and available publicly. The two keys are secret. The

4 Some possible uses of the Bluetooth stack

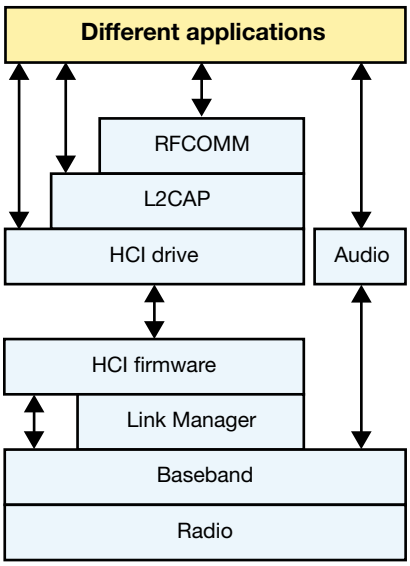


Table: The entities used in Bluetooth™ authentication and encryption

	Size
Bluetooth device address	48 bits
Private user key, authentication	128 bits
Private user key, encryption	8–128 bits
Random number	128 bits

authentication key is used when the link is established; the encryption key is used for encrypting user data. The variable-length encryption key facilitates a trade-off between the required security and the computational burden. Random numbers are used for the challenge-response scheme, for authentication, and for generating encryption keys.

Bluetooth in industry: opportunities and limitations

The Bluetooth technology opens up new possibilities for wireless communication in industrial environments due to its low cost and built-in security. Wireless communication has some inherent advantages and disadvantages, and ABB considers these carefully when utilizing wireless technology for industrial applications.

The main advantages of wireless communication are:

- No communication cables
- Flexible topology
- Possibility of mobile applications

Its main disadvantages are:

- Sensitive to interference (radio frequency shared with other devices)
- Security (confidentiality, integrity, message tampering, spoofing, privacy)
- Denial of service (jamming)

In order to benefit from the advantages of mobility and the removal of all wires, the power supply issue has to be resolved. Since, in some applications, power might be supplied locally for other purposes, it is possible to power the wireless units from this source as well. However, many applications require the complete removal of cables and so power must be obtained by other means, eg battery, local generation, solar panels, etc.

Bluetooth also has some advantages and disadvantages compared with wireless in general. The main advantages are:

- Low cost, low power
- Built-in security

The main disadvantages of Bluetooth are:

- Bandwidth shared with other systems
- Short range (up to 100 meters)

Bluetooth links will be available universally and will allow industrial equipment to inter-operate with portable computers, palm tops and mobile telephones. The low cost of Bluetooth also opens up the possibility of introducing wireless in other industrial applications, such as sensing, data collection and monitoring.

Industrial applications are somewhat different from those for which Bluetooth was originally designed. The messages are often short, but it is important for the information to be transferred swiftly and securely. Time stamping of such messages is widely used. ARQs could be undesirable in some applications where additional information is available for deciding whether the packets should be retransmitted or if other action should be taken.

ABB Corporate Research in Norway has used Bluetooth for data collection in which the measurement equipment is controlled by a PIC micro-controller. The application that runs in the micro-controller performs measurements which are stored in the internal memory and are communicated via Bluetooth at regular intervals. The protocol used for the communication between the PIC controller and the Bluetooth module is the Host Controller Interface (HCI). The small PIC controller is more than capable of handling the communication with the Bluetooth module, in addition to collecting measurements and calculating the results.

Industrial equipment is often installed in harsh environments with extreme temperatures, vibration, etc. The Bluetooth module used in industry should be able to withstand –40°C to +80°C and be of robust design.

The Bluetooth module in the above-mentioned data collector has undergone severe testing to verify its ability to operate in a harsh environment, eg tests simulating lightning 5, which can cause problems if the antenna signal is not carefully filtered.

Power consumption is also a major issue since power is not normally available. A battery solution has the drawback that the benefit of introducing wireless is compromised when personnel have to replace batteries regularly.

Radiowave propagation in industrial environments

ABB Corporate Research Norway has undertaken various measurements of radiowave propagation in industrial environments. A transmitter transmitting a continuous unmodulated carrier and IEEE 802.11 compliant equipment that uses the same frequency band as Bluetooth have been investigated. The 802.11 equipment uses direct sequence spread spectrum as opposed to the frequency hopping used in Bluetooth. The overall performance of the two radios in industrial environments is considered to be similar to that of Bluetooth.

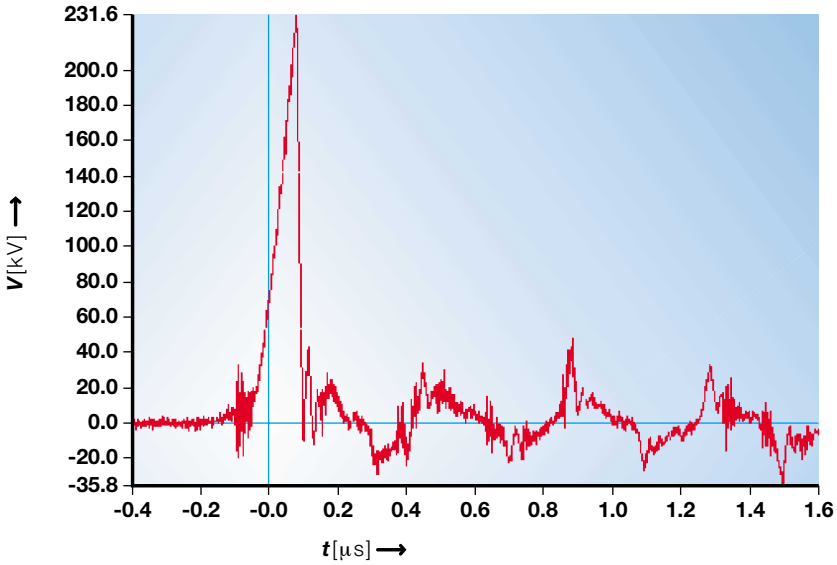
Measurements were made at three different sites: a cable production hall, a pulp mill, and a nuclear power plant. Machinery and large concrete structures were present at all three sites.

The measurements showed that the received signal consisted of a large number of components which had been reflected off walls and machinery and had traveled by different paths from the

5 Lightning test voltage

V *Voltage amplitude*

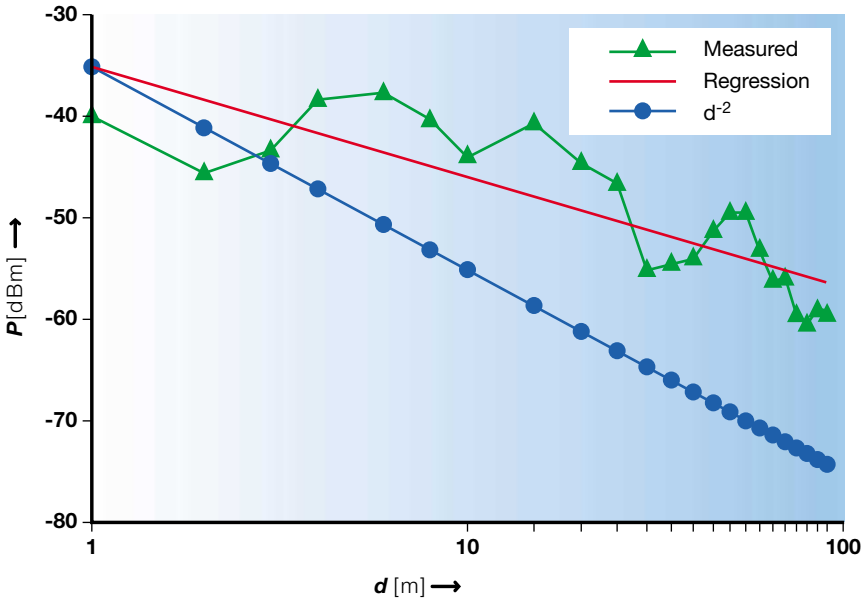
t *Time*



6 Received power in a pulp mill

P *Received power*

d *Distance between transmitter and receiver (log)*



transmitter to the receiver. This effect leads to very rapid variations in the received signal strength and can cause severe problems for radio communication equipment that is not set up for multipath environments. On the other hand, the reflections provide radio coverage in areas where there is no line of sight between the transmitter and receiver. The reflections also reduce the average path loss.

The test results show that the received power, averaged over one wavelength to avoid fast fading effects, is proportional to $d^{-1.1}$, where d is the distance between the receiver and transmitter 6. The attenuation is therefore significantly lower than in free space, where the received power is proportional to d^{-2}. In addition, no problems due to fast fades were encountered. This shows that the direct sequence spread spectrum technique used in this equipment is resistant to multipath fading and that the multipath environment is more friend than foe for this type of equipment.

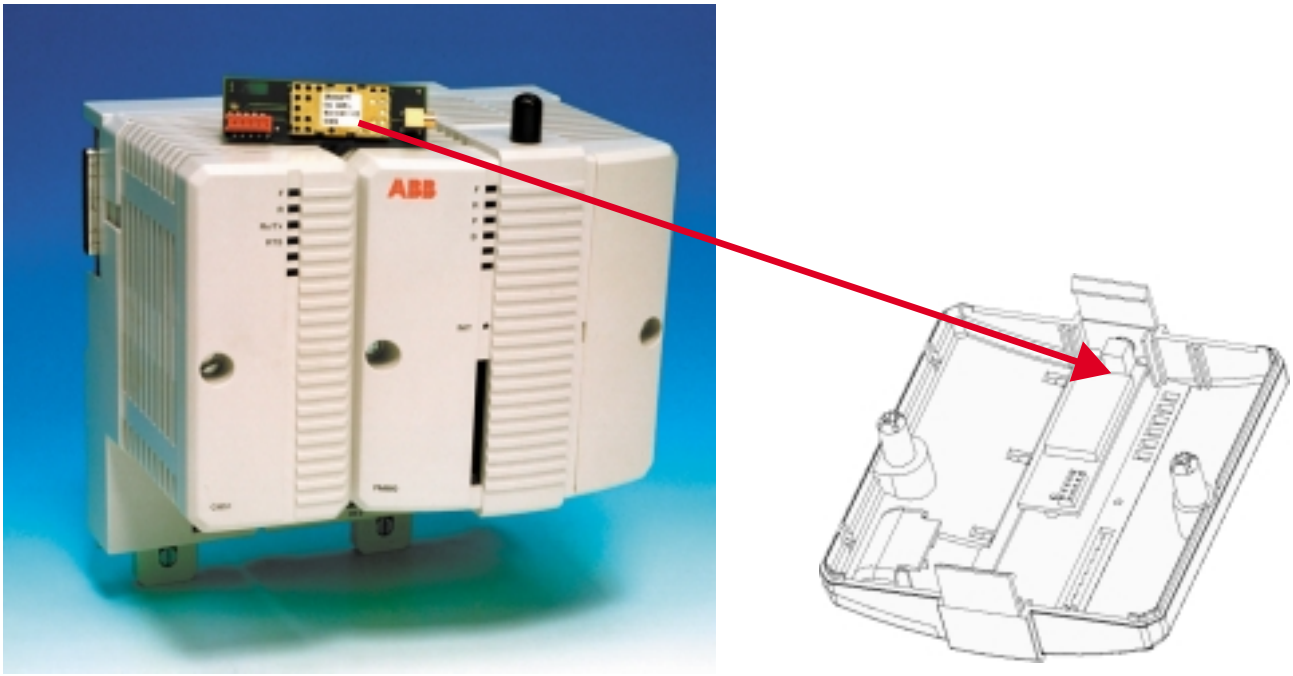
What is more, frequency hopping spread spectrum is resistant to multipath fading. The above results are considered to be valid for Bluetooth equipment.

Bluetooth – part of the ABB Advant AC800 controller

A new generation of industrial controllers developed by ABB Automation Products in Sweden needs communication for system engineering, installation, and maintenance. The communication link must be robust and inexpensive. Infrared communication has been investigated, but it has serious shortcomings since line of sight is required. A radio solution would not only overcome such problems but also be more flexible.

ABB Corporate Research Norway has used Bluetooth technology to replace the serial RS232 cable connecting the PC/NT running the Advant Control Builder application to the AC800 controller. This gives easy access to the controller in the field. 7 shows a picture of the AC800 controller with the

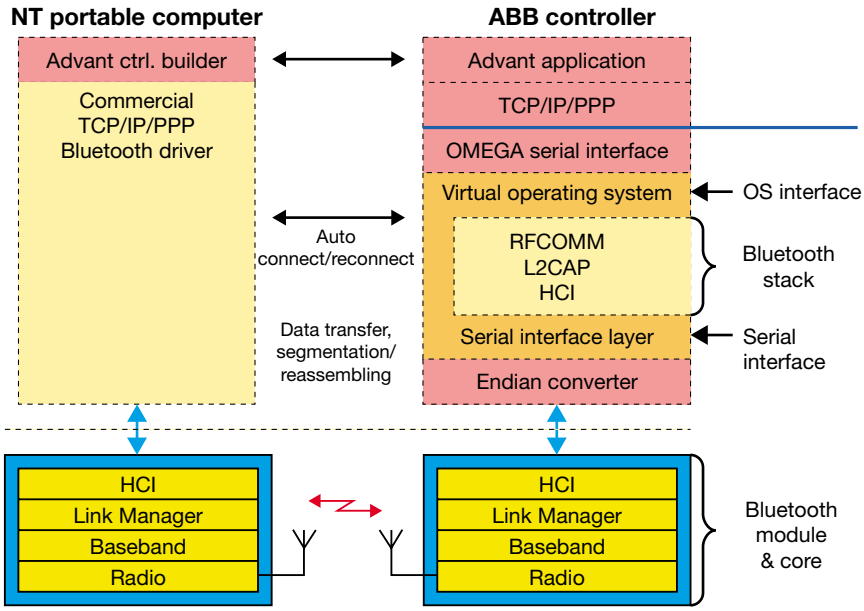
7 Bluetooth radio integrated in an Advant Controller



Bluetooth module integrated in the housing.

At the Interkama fair in October 1999, ABB Automation Products became the first industrial automation company in the world to demonstrate an industrial application using a Bluetooth link. This application allows seamless integration of ABB controllers with office-automation equipment. It offers a short-range link providing a flexible and reliable data connection for support of installation, commissioning and maintenance tasks.

The software approach was to enable the controller to use Bluetooth for the RS232 serial communication. On the NT platform an NT kernel driver was developed that handles the Bluetooth protocol. This driver is located above the NT serial driver but still in the kernel mode, such that the WIN32 API for serial communication could still be used and required no changes to the PC/NT application 8.



8 The Advant protocol stack

Summing up

Bluetooth looks set to become a new global standard for short-range radio. Its main advantages are its low cost, broad support from vendors and the fact that it operates in the unlicensed ISM frequency band. ABB Corporate Research Norway has considerable experience in using Bluetooth and the software stack. The problems encountered have been relatively minor, especially when it is considered that Bluetooth is still in its early stages.

ABB has tested communications in the ISM frequency band (2.4 GHz) in industrial environments, and fewer difficulties were encountered than might have been expected. Rapid fading from multipath is an issue that still has to be dealt with, but this is offset by the better coverage and lower path losses.

Authors

Jan Endresen
Torkil Brunsvik
Håkon Beckman
Snorre Kjesbu
ABB Corporate Research
Bergervein 12
NO-1361 Billingstad/Norway
jan.endresen@no.abb.com
Telefax: +47 66 84 35 41

References

[1] Specification of the Bluetooth System - Core, v.1.0 B, Dec 1999. www.bluetooth.com

[2] The Bluetooth Story: www.bluetooth.com

[3] Specification of the Bluetooth System - Profiles, v.1.0 B, Dec 1999. www.bluetooth.com.