Published October 1, 2003. Distribution restricted to Sponsors until January 1, 2004.

AUTO-ID CENTRE

# WHITE PAPER

## Demystifying RFID: Principles & Practicalities

Steve Hodges & Mark Harrison

AUTO-ID CENTRE INSTITUTE FOR MANUFACTURING, UNIVERSITY OF CAMBRIDGE, MILL LANE, CAMBRIDGE, CB2 1RX, UNITED KINGDOM

## ABSTRACT

This paper provides an insight into the operation of the radio frequency identification (RFID) component of the EPC™ network. It is aimed at a non-technical audience, in particular those wishing to deploy EPC™ network applications within their organisations. It will provide this audience with an understanding of how such applications will operate at an RFID level.

Issues that are covered include the physics of operation of radio communications systems in general and of RFID in particular, the different types of RFID system that are available, legislation regarding the use of RFID around the world and standardisation efforts in this area.

This paper is based on a Cambridge University internal report with the same title [10]. However, the original information sources, which are believed to be the most up-to-date at the time of writing, are cited as appropriate.

Feel free to contact the authors for more details on any of the areas discussed or for subsequent, more up-to-date information.

Published October 1, 2003. Distribution restricted to Sponsors until January 1, 2004.

# WHITE PAPER

## Demystifying RFID: Principles & Practicalities

## Biographies

**Steve Hodges**
Technical Director
seh@eng.cam.ac.uk

Steve Hodges is the Technical Director of the Auto-ID Centre, Europe, based at the Cambridge Lab. Steve has a strong technical background with a first degree in Computer Science with Electronic Engineering, from University College London, and Ph.D. from Cambridge University Engineering Department in the area of Robotics and Computer Vision.

As the Technical Director at the Auto-ID Centre, Steve can use his detailed understanding of all facets of the technology to help deliver lucid education programmes to industry and to provide independent advice to those wishing to deploy Auto-ID technology.

**Mark Harrison**
Senior Research Associate
mark.harrison@cantab.net

Mark Harrison is a Senior Research Associate at the Auto-ID Centre lab in Cambridge working on the development of the EPC™ information service (EPCIS), as well as web-based graphical control interfaces and manufacturing recipe transformation ideas. In 1995, after completing his PhD research at the Cavendish Laboratory, University of Cambridge on the spectroscopy of semiconducting polymers, Mark continued to study these materials further while a Research Fellow at St. John's College, Cambridge and during 18 months at the Philipps University, Marburg, Germany. In April 1999, he returned to Cambridge, where he has worked for three years as a software engineer for Cambridge Advanced Electronics/Internet-Extra, developing internet applications for collaborative working, infrastructure for a data synchronisation service and various automated web navigation/capture tools. He has also developed intranet applications for his former research group in the Physics department and for an EU R&D network on flat panel displays.

# WHITE PAPER

## Demystifying RFID: Principles & Practicalities

## Contents



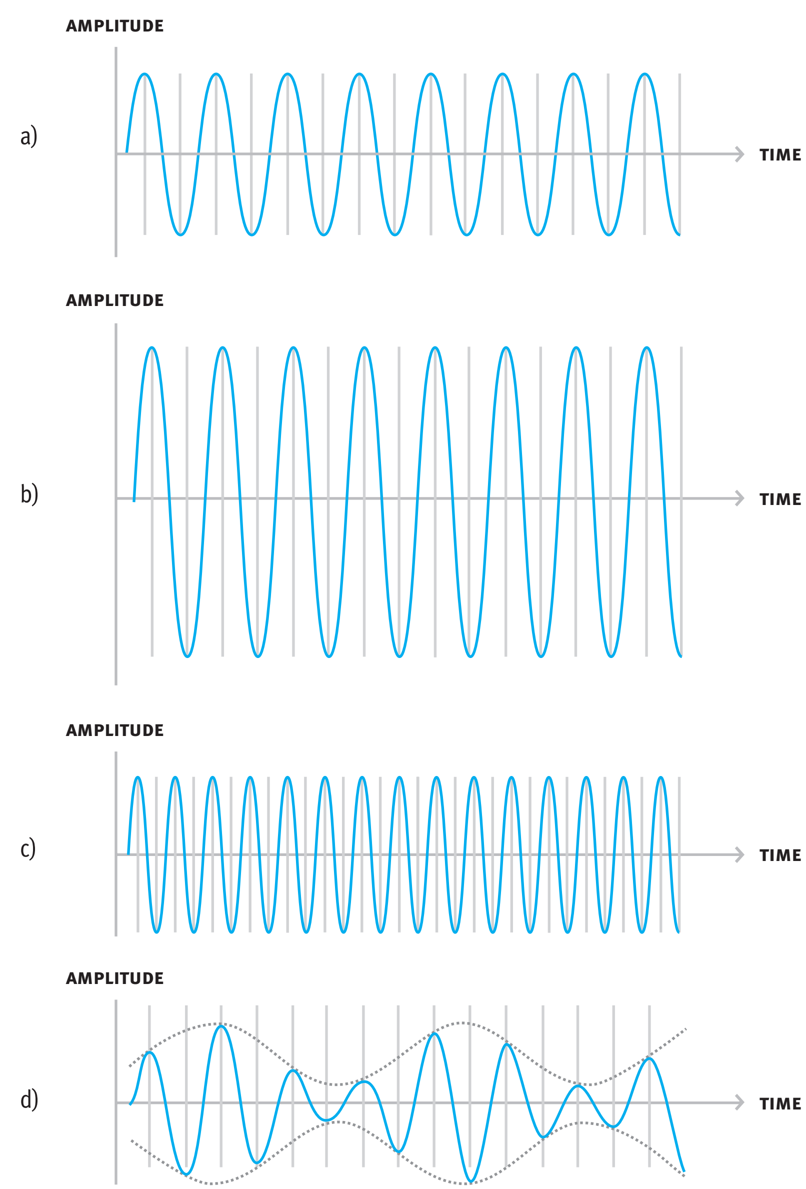
# 1. THE PHYSICS OF RADIO COMMUNICATION

## 1.1. Electromagnetic Radiation and the Electromagnetic Spectrum

In the 19th Century, James Clerk Maxwell formulated equations describing how energy could be transmitted from one place to another, through a principle that was later to become known as the **propagation of electromagnetic (EM) radiation** [7]. The easiest way to understand how this works is to consider a wave of energy that emanates from a source (the **transmitter** of EM radiation), see Figure 1a.

**Figure 1a, 1b, 1c & 1d:** Representing electromagnetic radiation as a wave of energy. a) shows a basic wave, whilst the wave depicted in b) has double the amplitude (ie. is more powerful) and that in c) has double the frequency. The wave in d) demonstrates how the amplitude of a wave may be altered continuously.

**ELECTROMAGNETIC RADIATION REPRESENTED AS A WAVE**



It is possible to control the nature of the electromagnetic wave in a number of ways. For example, a more powerful transmission will result in a bigger wave (technically, this is called a larger **amplitude**) – see Figure 1b. It is also possible to increase or decrease the rate at which the wave oscillates (see Figure 1c for example) – technically, the rate of oscillation is known as the **frequency** of the wave. As you may imagine, it is also possible to vary the amplitude or the frequency of the wave (or even of both) as time goes on, which leads to more complex waveforms – see Figure 1d for example (Section 1.3 gives more details on this concept). Frequency is measured in **Hertz** (Hz), or more commonly kilohertz (kHZ), megahertz (MHz) or gigahertz (GHz) (see Table 1).

**Table 1:** Scientists use various forms of notation for representing large frequencies.

**THE RELATIONSHIP BETWEEN KILOHERTZ, MEGAHERTZ AND GIGAHERTZ**

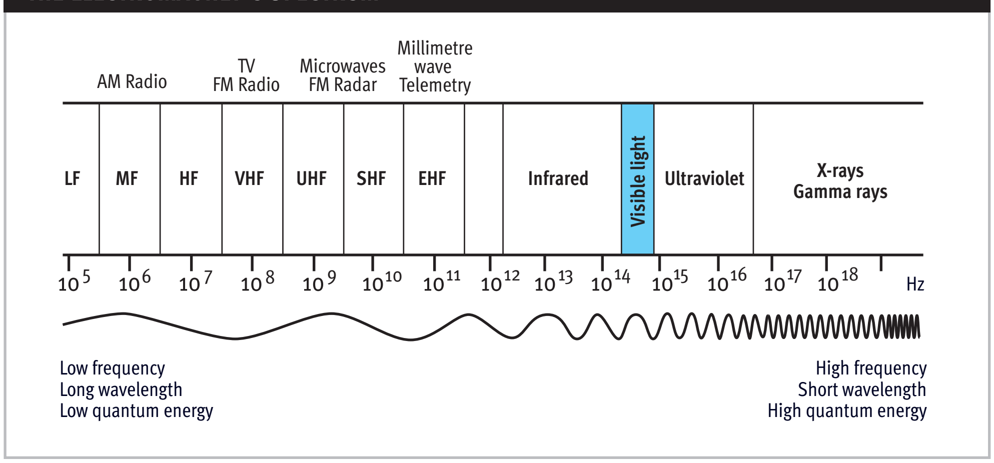
| | | | | | |
|---|---|---|---|---|---|
| **kilohertz** | 1kHz | = 1,000 Hz | = $10^3$ Hz | | |
| **megahertz** | 1MHz | = 1,000 kHz | = 1,000,000 Hz | = $10^6$ Hz | |
| **gigahertz** | 1GHz | = 1,000 MHz | = 1,000,000 kHz | = 1,000,000,000 Hz | = $10^9$ Hz |

The frequency of an electromagnetic transmission is particularly interesting. In turns out that an absolutely huge range of frequencies are possible, and the characteristics of the transmission vary greatly with the frequency used. Whilst similar frequencies have similar properties, moving across this spectrum of electromagnetic frequencies (known as the **electromagnetic spectrum**) results in dramatic changes in properties such as the ability of the wave to pass through different materials.

To help characterise these different properties, physicists segmented the electromagnetic spectrum into different regions (or **bands**) – with the idea being that within a particular band, the properties would be similar because the frequencies are similar. These bands are only a rough way of referring to the spectrum – often a larger or a smaller range of frequencies is relevant and in this case it may be appropriate to refer to a number of bands or just to part of a single band. The EM spectrum and the bands are shown in Figure 2.

**Figure 2**

**THE ELECTROMAGNETIC SPECTRUM**




As can be seen from Figure 2, one of the bands is the a set of frequencies that are visible to the human eye. Put another way, human vision relies on the ability of the eye to detect electromagnetic radiation with a certain range of frequencies – the range known as **visible light**. Red light has a different frequency compared to blue light – and as a result these have slightly different properties (red light doesn't affect photographic film in the same way that blue light does for example); but because the frequencies of red and blue light are very similar, they generally have similar behaviours.

## 1.2. Radio Waves

Just as there is a narrow range of frequencies of electromagnetic (**EM**) propagation that we refer to as visible light, there is also a wider range of frequencies, from around 300kHz to 3GHz, which share certain characteristics and are referred to as **radio waves**.

The frequencies of the different bands of the EM spectrum that are considered to be radio waves are listed in Table 2. Note that the **UHF** band technically refers to any frequency within the range of 300MHz to 3GHz, which clearly includes 2.5GHz, the frequency of microwaves. However, sometimes 'UHF' is used to refer to a smaller band that actually excludes microwaves.

**Table 2:** The exact definition of the bands within the radio wave portion of the electromagnetic spectrum.

**RADIO WAVE BANDS**

| **Band designation** | **LF** low frequency | **MF** medium frequency | **HF** frequency | **VHF** very high frequency | **UHF** ultra high frequency | **SHF** super high frequency |
|---|---|---|---|---|---|---|
| **Frequency** | 30–300kHz | 300kHz–3MHz | 3–30MHz | 30–300MHz | 300MHz–3GHz | 3–30GHz |
| **Wavelength** | 10–1km | 1000–100m | 100–10m | 10m–1m | 1m–0.1m | 0.1–0.01m |

## 1.3. Radio Wave Transmission and Reception

There are different ways of creating an electromagnetic wave (lighting a fire causes visible light to be emitted, for example), but radio waves are typically generated by electronic circuitry connected to an aerial (or, more properly, an **antenna**). That electronic circuitry can usually control, to a small extent, the frequency and the amplitude of the wave that it generates. An external (electrical) power source is needed to provide the energy to transmit the radio wave. And since electronic components are never 100% efficient, not all the power provided to the circuit will be passed through to the radio transmission.

It is particularly useful for a radio transmitter to vary the nature of the wave being transmitted to a small extent. By doing this continuously, it becomes possible to represent (or **encode**, or **modulate**) information within the radio transmission. At the simplest level, one can imagine a Morse-code like system where the transmitter switches on and off to represent different letters in a particular transmission. However, it is also possible to use much more sophisticated schemes, where the frequency and/or amplitude of the transmitted wave are varied subtly to encode a great deal of information. (Figure 1(d) showed a very simple example where the amplitude may be varied – a process called **amplitude modulation**).

Radio waves may be **received** in an analogous way, by an antenna connected to an electronic circuit. It is possible to build a receiving system in which no external power is required – all the energy for operating the electronics is derived from the radio wave that is being received. This is exactly the mechanism used by crystal radio sets, for example. However, radio receivers usually do use an external power source such as a battery or mains power. In both cases, the ultimate aim of the receiver is to decode the information that is being transmitted, in order to pass it on to some subsequent part of the electronic system.

Of course, in order for a radio receiver to make sense of the radio waves it receives, it must know the way in which information has been encoded by the transmitter. This is known as the **physical layer protocol**, or sometimes as the **air interface** of the system.

**RADIO COMMUNICATION SYSTEM**

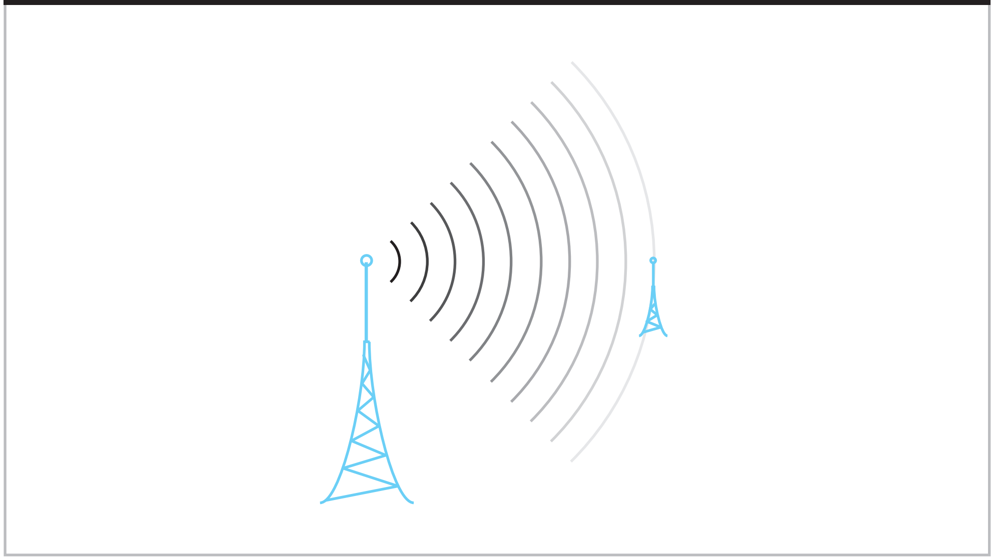


**Figure 3:** A radio communication system, with a transmitter (on the left) and a receiver (on the right). The transmitter generates the electromagnetic wave, some of which will be incident on the receiver.

## 1.4. The Range of a Radio Communication System

For any given radio transmitter and receiver, there is a maximum distance (or **range**) over which communications can work reliably. If the separation between transmitter and receiver in increased beyond this distance, the receiver will no longer be able to correctly recreate the information being transmitted. It is prudent to operate a radio communications system with a certain **margin**, i.e. not right at the maximum range, since the exact range is likely to change from moment to moment and this must be accommodated to achieve reliable performance.

The exact range will be affected by a number of factors, but in simple terms there are four:

1. the power contained in the wave transmitted
2. the **sensitivity** of the receiving equipment
3. the environment through which the wave travels
4. the presence of **interference**

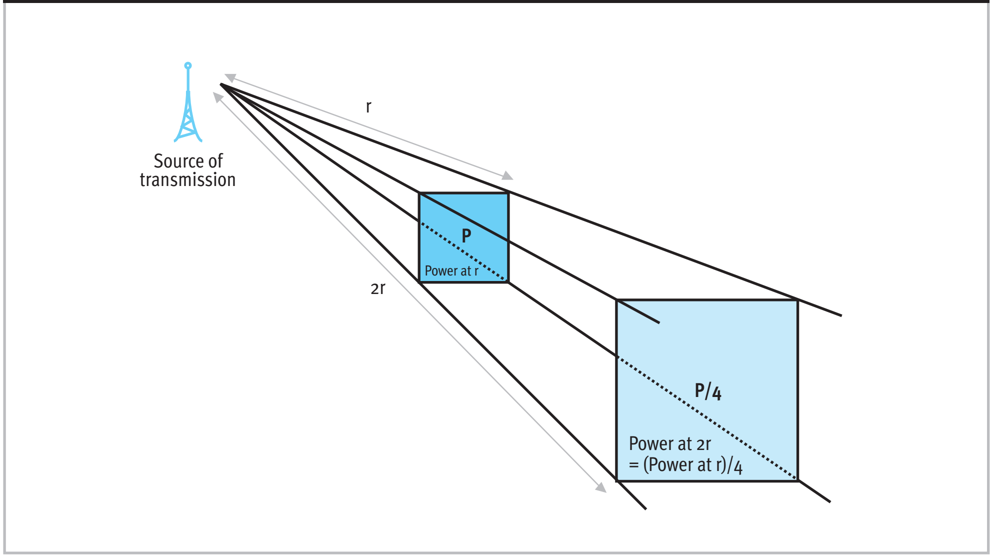
These are largely self-explanatory, but of particular note is the relationship between power and distance. As the radio wave travels away from the transmitting antenna, it disperses in all directions. This means that every time the distance from the transmitter doubles, the proportion of the original wave that is available for reception is quartered. This so-called inverse square relationship is illustrated in Figure 4.

Also note the effect that the environment has on radio communication. When electromagnetic radiation passes through materials, it may be absorbed to a certain extent, depending on the properties of the material and the type of radiation. This absorption results in a reduction of the strength of the radiation, a process known as attenuation. This **attenuation** increases with the thickness of the material.

Visible light is absorbed relatively easily, whereas radio waves are more likely to pass through materials (especially gases in the atmosphere, such as nitrogen and oxygen, and also paper, cardboard and certain plastics) with only little attenuation of the radiation. Other materials (metal and liquids, for example) have a stronger attenuating effect, although such attenuation varies depending on the frequency of the wave. Once again, the different frequencies within a single band will display similar properties to each other.

**Figure 4:** If the distance from the transmission source is doubled (from 'r' to '2r'), then the same amount of energy is now spread over four times the area. This means that the power available at any one point is quartered.

**THE INVERSE SQUARE LAW**




In addition to attenuation by absorption, certain frequencies of radio waves are also susceptible to something known as **multipath** interference. This occurs when waves are reflected by objects in the environment, and the reflections interfere with the original waveform. This makes it much more difficult for the radio wave receiver to determine the original wave, and in the worst case there are positions (called **nulls**) where reception is not possible even though the transmitter and receiver are relatively close to each other.

Similarly, if there are any other radio waves being transmitted on a similar frequency, then these will cause interference in the same manner.

## 1.5. Antennas and Wavelength

As already mentioned, the antenna is a critical part of a radio communications system. The size, shape and specific properties of an antenna will depend very much on the frequency of the wave that is to be transmitted or received.

In general, the size of the antenna is proportional to the **wavelength** of the radio wave. Wavelength is essentially just another way of representing the frequency of a radio wave. Whilst frequency is measured in Hertz, wavelength is just that – a length – and is therefore measured in metres. Large frequencies are equivalent to small wavelengths and vice versa – Table 2 includes some examples.

Note that an antenna is typically most effective at a single frequency (the **centre frequency**) – it will not work as well at frequencies above and below this. However, at a given frequency the same antenna can be used equally well for transmitting radio waves or for receiving them.

Different types of antenna have different **radiation patterns**, i.e. the directions in which they can transmit or receive electromagnetic radiation. Many antennas are **directional**, which means that they work best in a certain orientation.

In addition to the directional aspect of the radiation pattern, antennas may produce radiation that is **linearly polarised** or **circularly polarised**. The main point to bear in mind relating to the type of polarisation is that in the case of linear polarisation, the transmitting and receiving antennas must be parallel with each other in order to maximise the strength of the received signal. Circularly polarised antennas do not have this restriction – the relative orientation of the two antennas is less critical.

## 2. RADIO FREQUENCY IDENTIFICATION

Radio frequency identification (commonly abbreviated to **RFID**) is so-named because it relates to the identification of objects using EM radiation at radio frequencies.

In Table 2 we saw that a large range of frequencies within the EM spectrum are referred to as radio frequencies (**RF**), which results in a number of different forms of RFID. Once again, RFID systems may be categorised based on the band of the EM spectrum that they operate in. RFID systems in the same band will generally display similar characteristics; those in other bands may well operate very differently and therefore be more or less suitable for a given application.

### 2.1. The Basic Operation of an RFID System

An RFID system comprises two components – an RFID reader and an RFID tag. Despite its name, the RFID reader is really the transmitter in an RFID system. The electronics in the reader uses an external power source to generate the signal that drives the reader's antenna and which in turn creates the appropriate radio wave. This radio wave may be received by an RFID tag, which in turn 'reflects' some of the energy it receives in a particular way (based on the identity of the tag). Whilst this reflection is going on, the RFID reader is also acting as a radio receiver, so that it can detect and decode the reflected signal in order to identify the tag. This process is depicted in Figure 5.

**THE PRINCIPLE OF OPERATION OF AN RFID SYSTEM**

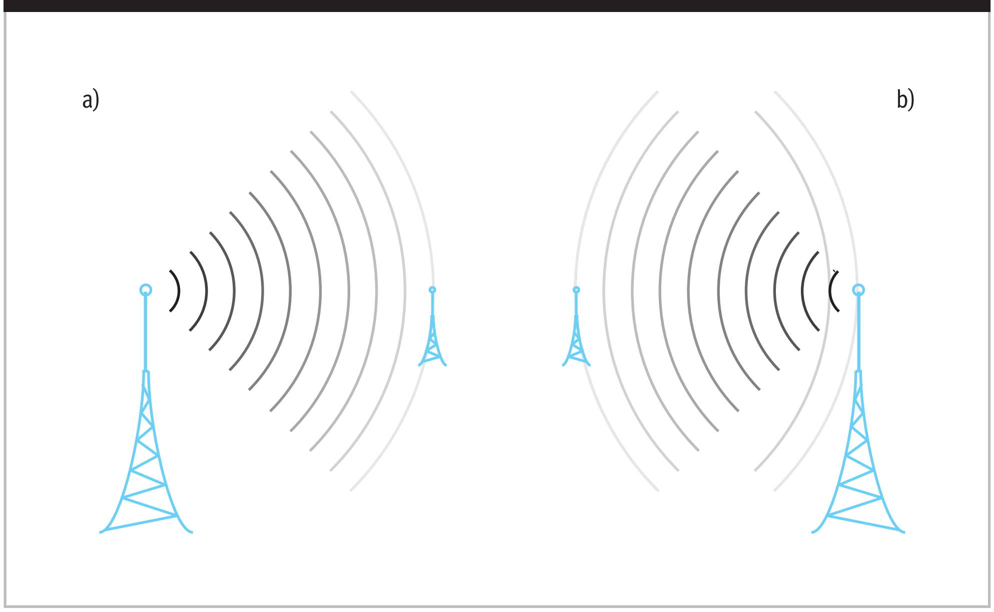



**Figure 5:**

a) The RFID reader (left) initially transmits a radio wave, which is used to power the RFID tag (right).

b) The tag selectively reflects energy back to the reader, which is now acting as a receiver, in order to communicate its identity.

An RFID system is specifically designed to be asymmetric – the reader is big, expensive and power hungry compared to the RFID tag. There are a number of different types of RFID system, but one basic categorisation is based on the power source used by the tag:

1. **Passive tag RFID systems** require no power source at the tag – there is no battery. Instead, the tag uses the energy of the radio wave to power its operation, much like a crystal radio. This results in the lowest tag cost, but at the expense of performance.
2. **Semi-passive tag RFID systems** rely on a battery built into the tag in order to achieve better performance (typically in terms of operating range). The battery powers the internal circuitry of the tag during communication, but is not used to generate radio waves.
3. **Active tag systems** use batteries for their entire operation, and can therefore generate radio waves proactively, even in the absence of an RFID reader.

Passive tag RFID systems are the most common type, and are often referred to simply as 'RFID systems'.

## 2.2. Range of RFID Systems

With an RFID system, the term **range** naturally refers to the maximum operating distance between the reader antenna and the tag, and the **field** of the reader is the specific operating area.

The frequency of operation used for an RFID system has a big effect on the operating range. Analysis of the physics of RFID communications shows that the optimum frequency is around 400-500MHz [9]. Such analysis cannot be made generically - there are a number of factors to take into account and these will have different effects based on the intended application. Example factors that will be affected by the choice of frequency include: size of tag antenna, ease of power delivery to the tag, ease of communication of tag back to reader, cost and speed of communication.

The range of RFID systems operating in the UHF band is governed largely by the principles outlined in Section 1.4. This means that the ability of the reader to power and communicate to the tag is based on the inverse square law ($1/r^2$), as will the **return path** of reflected signals from the tag to the reader. Operation will also be affected by environmental conditions and interference from other radio sources at the same frequency.

RFID systems that operate in the HF band of the spectrum work in a very different way to those using the UHF band and it is useful to understand this fundamental difference and the effect it has on operating range. If communication occurs over a short distance, relative to the wavelength of the radio wave, this is said to be **near-field** operation. Since HF (3-30MHz) RFID systems use waves with a wavelength of around 10-100m, if the distance of the communication is much less than this (which is the case in RFID) then this is a near-field communication. Near-field communication is based on a magnetic field effect, which has an inverse sixth power ($1/r^6$) relationship with range.

Of course, if a directional antenna is used, its radiation pattern will also affect the reader field.

## 2.3. Reading Multiple Tags

One of the advantages of RFID systems over barcodes and other identification techniques that is often cited, is the ability of an RFID system to identify multiple tags in the field of a reader simultaneously. In fact, identification of multiple tags in this way is very rarely performed truly simultaneously – more often the tags are identified (or **singulated**) consecutively, albeit in a very short time. In order that the tags don't interfere with each other, some kind of mechanism must be built into the way in which the RFID system operates – this is known as an **anticollision protocol** because it prevents the responses from the different tags from colliding with each other. There are different ways of building an RFID system that uses anticollision. Most often the reader is responsible for preventing collisions (i.e. the reader **arbitrates** between the different tags), a technique known as **reader talks first**.

Depending on the protocol used by an RFID reader, the rate at which different tags in the field can be identified (the **read rate**) will vary. Read rate is often expressed in terms of the number of **tags per second** that may be identified, but it is important to understand that this figure may be misleading. It may be possible for an RFID system to read the identity of a single tag many hundreds of times over in a second, but that same system may not be able to read several hundred different tags in one second. What is often significant in real applications is the time taken to identify all of the tags in the field, or the **time to last tag**.

### 2.4. Using Multiple Readers

In many applications, it will be necessary to install several RFID readers in reasonably close proximity to each other. As a result, they may well be in range of each other – i.e. they have the potential to interfere with each other. (Since an RFID reader is designed to receive the tiny signal reflected from a tag, it will be particularly susceptible to any (relatively powerful) transmissions from other readers that happen at the same time.) It is also likely that the frequency band in use is shared with other potential users, which may again cause interference (see Section 4).

One of two different mechanisms is often used to prevent such interference. The first, known as **spread spectrum**, works by spreading a radio transmission across a reasonably wide band of different frequencies in a special way, such that multiple simultaneous transmissions (by different systems, for example) will end up using different parts of the radio spectrum and will therefore be able to operate largely without effect on each other. There are in fact two popular variants of this technique, called **frequency hopping** and **direct sequence** spread spectrum (**FHSS** and **DSSS** respectively).

The second mechanism, which is proposed for use in Europe and is likely for use in Japan as well (where the narrower band allocation outlined in Section 4.5 makes spread spectrum less attractive), is known as **listen before talk**, or **dynamic frequency selection** [1].

## 3. LEGISLATION REGARDING THE USE OF RFID

### 3.1. The Role of Legislation and Spectrum Regulation

Because of the value of communication, the EM spectrum is a valuable resource that is controlled by governments around the world. At some frequencies the transmission of EM waves has a very limited/localised effect. Visible light, for example, is easily attenuated and blocked. However, radio waves are considerably more pervasive – a transmitter in one building/town/country can have a significant impact on the operation of a receiver in another building/town/country. Therefore, the transmission of radio waves is typically controlled quite tightly by national and international treaties. They specify the amplitudes, frequencies, communication mechanisms and applications that are permitted through a process known as spectrum licensing.

## 3.2. Legislation Regarding RFID in General

There are a number of frequency ranges in which the operation of RFID systems is permitted. Unfortunately, because national governments have historically been responsible for spectrum licensing, different countries often have different frequency allocations. Governments around the world have been working for many years to harmonise their spectrum allocations, and this work will inevitably be on-going. However the current status with regard to RFID is that in most regions of the world you can use an RFID system in the LF, HF or UHF parts of the spectrum. LF and HF operation is very similar across different regions, but UHF operation varies from region to region. These differences relate to the specific frequencies and power levels that are allowed, the speed at which communication can occur, the range of uses that a band is shared between, and the ways in which such sharing is enforced.

Many governments recognise the potential utility of RFID systems, and the value of harmonised radio communication systems in general, and as a result are actively working to ensure that (a) sufficient spectrum is allocated within their own region and that (b) differences between different regions are minimised (if not eliminated).

## 3.3. Specific Legislation at LF

**125 – 134kHz**
This frequency is available for use for RFID systems in Europe, North America and Japan.

## 3.4. Specific legislation at HF

**13.56MHz**
This frequency is available for use for RFID systems Europe, North America, Australia and Japan at very similar power levels.

## 3.5. Specific Legislation at UHF (Non-Microwave)

**865.6 – 867.6MHz**
There is a draft recommendation for extension to the unlicensed 869.4-869.65MHz European band which would allow transmission at up to 2W ERP (equivalent to 3.2W EIRP) using ten 200kHz channels. NB this draft also allows transmission of up to 0.1W ERP between 865.0MHz and 865.6MHz, and at up to 0.5W ERP between 867.6MHZ and 868.0MHz; however, these allocations are unlikely to be used for RFID in practice.

**869.4 – 869.65MHz**
Currently there is a very small (250kHz) unlicensed allocation in Europe that may be used for RFID (along with other applications), at up to 0.5W ERP. This has been used by some RFID systems, but performance is limited.

**902 – 928MHz**
Unlicensed band available for use in North America by systems deploying spread spectrum transmission at up to 4W EIRP. This band must be shared with other (non-RFID) users observing the same frequency hopping rules, such as wireless LAN systems.

**918 – 926MHz**
Australian allocation available for RFID, up to 1W EIRP.

**950 – 956MHz**
Potential allocation for RFID in Japan, following the decommissioning of the Japanese personal digital cellular mobile phone service in March 2002. The Japanese MPHPT (Ministry of Public Management, Home Affairs, Posts and Telecommunications) plan to study the feasibility of using this band for RFID and determine the necessary regulations regarding use of the band over the next 18 months or so. These regulations, which would reserve the band exclusively for RFID, could then possibly be adopted by March 2005 [1,2,6].

## 3.6. Specific Legislation at UHF (Microwave)

**2.45GHz**
Unlicensed band available in most regions of the world by systems deploying spread spectrum transmission, although the exact details of usage vary from region to region. Transmission at up to 4W EIRP is typically allowed (1W EIRP in Japan [2]). This band is used by IEEE 802.11b and 802.11g wireless LAN systems and Bluetooth communications systems, amongst others.

## 3.7. Operating Outside the Allocated Spectrum

In many jurisdictions it may be possible to obtain special permission from the regulators of the radio spectrum, in order to use equipment that operates outside the prevailing legislation. For example, the testing and development of new forms of RFID equipment, or the temporary use of non-compliant RFID equipment may be allowable, on a case by case basis. There are a large number of factors that will typically be taken into account in such circumstances, such as the location of the equipment to be deployed and the potential for interference with legitimate users of the spectrum.

This approach has been used by some companies in Europe wishing to start their RFID trials with equipment conforming to North American legislation. In these cases, the anticipated use of the non-compliant equipment is for a limited period and operation of the equipment has been modified to minimise the chance of it causing interference.

# 4. RFID STANDARDISATION

## 4.1. The Role of Standards in the RFID Industry

Traditionally, the RFID industry has been driven by diverse vertical application areas. In this environment, it is quite appropriate for different technology suppliers to develop RFID products to meet their perception of market needs, without any particular reference to the product offerings of their competitors. The products and the systems they result in must, of course, conform to the legislation that applies in the region in which they operate.

However, the lack of standardisation in the way in which RFID systems have been built has in recent years been recognised as a barrier to the more widespread adoption of the technology. Many applications require the interoperation of RFID products from different suppliers and/or of RFID systems in different regions. For this reason, there have in recent years been a number of attempts to create specifications that will standardise various aspects of the operation of an RFID system.

The rest of this section summarises the standards relevant to RFID that have been proposed by different industry bodies.

## 4.2. EAN.UCC

The **GTAG** (Global Tag) initiative was launched jointly by EAN International and the Uniform Code Council (UCC) in 2000. They recognised that the RFID industry was too fragmented and niche-oriented to serve the needs of their global user community [3].

The GTAG programme was designed to allow for both short-term solutions and the timely development of RFID standards based on identified business process requirements. These standards covered both UHF RFID technology (including air interface) and data formats, based on EAN.UCC's thorough understanding of business processes and how they can be improved [3].

The air interface efforts of GTAG have subsequently been merged with ISO 18000 part 6.

## 4.3. ISO/IEC JT1/SC17

The International Standards Organisation (ISO) is currently working with the International Electrotechnical Commission (IEC) to Address the standardisation of **Identification Cards and related devices**. This joint activity is being undertaken by JTC1/SC17 (Joint Technical Committee 1, Sub-committee 17). SC17 includes in its remit the standards 10536, 15693 and 14443.

**ISO/IEC 10536**
**Identification cards – Contactless integrated circuit(s) cards**
This standard describes the parameters for proximity coupling smart identification cards, with a typical range of 7-15cm, using RFID at 13.56MHz. There are four parts to the standard:

Part 1: Physical characteristics
Part 2: Dimensions and location of coupling areas
Part 3: Electronic signals and reset procedures
Part 4: Answer to reset and transmission Protocols

**ISO/IEC 14443**
**Identification cards – Proximity integrated circuit(s) cards**
This standard describes the parameters for proximity coupling smart identification cards, with a typical range of 7-15cm, using RFID at 13.56MHz. There are four parts to the standard:

Part 1: Physical characteristics
Part 2: Radio frequency Power and Signal Interface
Part 3: Initialisation and anticollision
Part 4: Transmission Protocols

**ISO/IEC 15693**
**Contactless integrated circuit(s) cards – Vicinity Cards**
This standard describes the parameters for vicinity coupling smart identification cards, with a typical range of up to 1m, using RFID at 13.56MHz. There are four parts to the standard:

Part 1: Physical characteristics
Part 2: Air interface and initialisation
Part 3: Protocols
Part 4: Extended command set and security functions

## 4.4. ISO/IEC JT1/SC31/WG4

ISO is also working with the IEC to address the standardisation of **Automatic Identification and Data Capture Techniques.** This joint activity is being undertaken by JTC1/SC31 (Joint Technical Committee 1, Sub-committee 31). One of the areas of consideration of SC31 is the use of **RFID for Item Management**, which is being undertaken by SC31/WG4 (work group 4). SC31/WG4 includes in its remit the standards 15961, 15962, 15963, 18000, 18001 [8].

**ISO/IEC 15961**
**RFID for Item Management – Data Protocol: Application interface**
(Previously named "RFID for Item Management – Host Interrogator – Tag functional commands and other syntax features", but name changed May 2003).

This standard defines common functional commands and syntax features (e.g. RFID tag-types, data storage formats, compression schemes etc.), independent of transmission media and air interface protocols. It is intended to be a companion standard to 15962, which provides the overall protocol for data handling.

The 15961 standard will comprise a super-set of all functional commands and other syntax features appropriate to RFID for item management. The 15961 functional commands are at a higher abstract level than those of the 18000 series, to enable common data handling rules independently of lower-level implementation.

**ISO/IEC 15962**
**RFID for Item Management – Protocol: Data encoding rules and logical memory functions**
(Previously named "RFID for Item Management – Data Syntax", but name changed May 2003)
This standard specifies the interface procedures used to exchange information in an RFID system for item management. The protocols established in this standard ensure the correct formatting of data, the structure of commands and the processing of errors in the RFID system.

**ISO/IEC 15963**
**RFID for Item Management – Unique Identification of RF Tag**
This standard specifies the numbering system, the registration procedure and the use of uniquely identifiable RFID tags. There are two parts; Part 1 covers the numbering system whilst Part 2 deals with the registration procedure and management guidance and rules.

The standard is designed to address three main aspects:

1. The traceability of the Integrated Circuit itself for quality control in their manufacturing process
2. The traceability of the RF tag during their manufacturing process and along their life in the applications where they are used
3. Anti-collision of multiple tags in the reader's field of view

**ISO/IEC 18000**
**RFID Air Interface Standards**
The ISO/IEC 18000 series of standards provide a framework to define common communications protocols for international use of RFID, and, where possible, to determine the use of the same protocols for different frequencies to minimise the problems of migration and to enable system management and control and information exchange to be common as far as is possible.

The ISO/IEC 18000 specifications are (currently) split into seven parts, summarised in Table 3. Part 1 describes the conceptual system architecture for RFID for item management and defines a common set of parameters that are necessary (at any frequency) in order to avoid contention or interference with other RFID systems, to establish as high a degree of interoperability as is practicable, and to ease integration with legacy systems. The subsequent parts of the standard provide the specific definitions for each of the approved frequencies, and where appropriate, provide regional definitions with geographical constraints.

Table 3

| ISO/IEC 18000 PARTS | |
|---|---|
| **Part 1** | Generic parameters for air interface communication for globally accepted frequencies |
| **Part 2** | Parameters for air interface communication below 125kHz |
| **Part 3** | Parameters for air interface communication at 13.56MHz |
| **Part 4** | Parameters for air interface communication at 2.45GHz |
| **Part 5** | Parameters for air interface communication at 5.8GHz (subsequently withdrawn due to lack of global acceptance) |
| **Part 6** | Parameters for air interface communication at 860–930MHz |
| **Part 7** | Parameters for air interface communication at 433MHz (late submission) |

Of particular interest are Parts 3 and 6. Part 3 has two different modes of operation, which are not interoperable although they are designed not to contend/interfere with each other. Mode 1 is based on ISO 15693 with improvements, whilst Mode 2 defines a new, high speed interface. Part 6 also defines two modes of operation, known as types A and B [5].

The ISO/IEC 18000 series of standards deals with only the air interface protocol and are not concerned with data content or the physical implementation of the tags and readers. These standards do not specify the data content or its structure, but are simply data carriers [4].

**ISO/IEC 18001**
**RFID for Item Management – Application Requirements Profiles (ARP)**

## 4.5. ISO/IEC JT1/SC31/WG3

JTC1/SC31/WG3 (Joint Technical Committee 1, Sub-committee 31, work group 3) deals with issues relating to conformance.

**ISO/IEC 18046**
**RF tag and interrogator performance test methods**
Working Draft (in committee). Preliminary Draft Technical Report expected late 2003.

**ISO/IEC 18047**
**RFID Device Conformance Test Methods**
This standard is split into a series of parts to mirror ISO/IEC 18000. Currently the various parts are in working draft format within their respective committees, with the exception of the part 3 (13.56MHz), which has progressed to the Preliminary Draft stage.

# 5. REFERENCES

1. **D. Weatherby, "EAN International and UHF Regulatory Standards as at September 2003".**
e.centre, September 2003.

2. **K. Morikawa, "Japan radio law's status including UHF band".**
(OMRON Corporation), Japanese SC31/WG4 Committee, August 29th, 2003.

3. **"Uniform Code Council and EAN International Announce Initiative for RFID Standards Development"**.
EAN.UCC Press release, March 17th 2000, available at
http://www.ean-int.org/pressreleases/ eanuccrfid.html

4. **C. Turner, "EPC and ISO 18000-6".**
RFID Journal article, March 2003, available at
http://www.rfidjournal.com/article/articleview/325/1/2/

5. **S. Halliday, "ISO/IEC 18000 – RFID Air Interface Standards".**
Feb 2003, available at
http://www.hightechaid.com/standards/18000.htm

6. **J. Murai, "Japan Opens Up UHF for RFID Use".**
RFID Journal Article, June 2003, available at
http://www.rfidjournal.com/article/articleview/477/1/1/

7. **R.A. Peters II, "A Brief Outline of the History of Electromagnetism".**
April 5, 2000; available at
http://www.vuse.vanderbilt.edu/~rap2/papers/em_history.pdf

8. **"ISO/IEC JTC1/SC31/WG4 homepage".**
http://usneto3.uc-council.org/sc31/sc31_wg4.cfm

9. **Personal communication from Peter Cole, 2003.**

10. **S. Hodges, "Demystifying RFID: Principles and Practicalities".**
Cambridge University Engineering Department, Technical Report CUED/E-MANUF/TR-028