CHAPTER 1

Technology Overview

Radio frequency identification (RFID) technology uses radio waves to automatically identify physical objects (either living beings or inanimate items). Therefore, the range of objects identifiable using RFID includes virtually everything on this planet (and beyond). Thus, RFID is an example of *automatic identification* (Auto-ID) technology by which a physical object can be identified automatically. Other examples of Auto-ID include bar code, biometric (for example, using fingerprint and retina scan), voice identification, and *optical character recognition* (OCR) systems.

Consider the word *identify* more closely. Although two cans, A and B, of a particular brand of motor oil in a store might look identical, substantial differences between the two might in fact exist. For example,

- The retailer might have used two different order numbers to obtain cans A and B from the distributor.
- Can A might have been produced in North America, whereas can B might have been manufactured in Asia.
- A person named Bob might have loaded A onto the delivery truck, whereas a person named Chi might have loaded B onto a similar truck.
- Can A might have arrived in the store on a different date than when can B arrived.

Generally, although none of the preceding information appears on cans A or B for a person to view in a store, this information is nonetheless associated with these cans. You can, by using a set of such information, uniquely identify can A from can B. Also, even assuming that no such information exists, the very fact that that two distinct physical objects exist suggests the possibility to distinguish them (for example, by assigning a number that is unique to can A and one that is unique to can B). In summary, although cans A and B might look identical in appearance,

composition, expiration date, recycling information, and so on, they can actually be differentiated in some way so that cans A and B, and any other can of motor oil produced by this particular manufacturer (or any other manufacturer), are *unique in some way*. When used in the context of RFID, the word *identify* refers to this uniqueness of an object.

The implications regarding object identity are tremendous. For example, consider how the preceding example of motor oil can be extended to other objects, irrespective of whether RFID technology can be used with:

- Every grain of rice consumed annually worldwide
- Every grain of sand on every beach worldwide
- Every leaf on every tree worldwide
- Every drop of rain that falls worldwide in a given year

The objects in this preceding list represent *potential* identification scenarios. Current RFID technology cannot be used to identify these objects. Even with technological advances (over the next 10 years, for example), some (or all) of these identification scenarios are unlikely. After all, how can you tag a raindrop, which has an extremely short life and dynamic behavior (such as dividing into smaller raindrops when it grows beyond 5 mm in size)?

Before delving into a detailed discussion of RFID technology, you need to understand the fundamental terms and concepts associated with RFID. The following section serves as an RFID technology primer.

1.1 Fundamental Concepts

A *wave* is a disturbance that transports energy from one point to another.

Electromagnetic waves are created by electrons in motion and consist of oscillating electric and magnetic fields. These waves can pass through a number of different material types.

The highest point of a wave is called a *crest*, and the lowest point is called a *trough*.

The distance between two consecutive crests or two consecutive troughs is called the *wavelength*.

One complete wavelength of oscillation of a wave is called a *cycle*.

The time taken by a wave to complete one cycle is called its *period of oscillation*.

The number of cycles in a second is called the *frequency* of the wave. The frequency of a wave is measured in *hertz* (abbreviated as Hz) and named in honor of the German physicist Heinrich Rudolf Hertz. If the frequency of a wave is 1 Hz, it means that the wave is oscillating at the rate of one cycle per second. It is common to express frequency in KHz (or kilohertz = 1,000 Hz), MHz (or megahertz = 1,000,000 Hz), or GHz (or gigahertz = 1,000,000,000 Hz).

Amplitude is the height of a crest or the depth of a trough from the undisturbed position. The former is also called the *positive amplitude*, and the latter the *negative amplitude*. In general, the *amplitude at a certain point* of a wave is its height or depth from the undisturbed position, and is called positive or negative accordingly.

Figure 1-1 shows several parts of a wave.

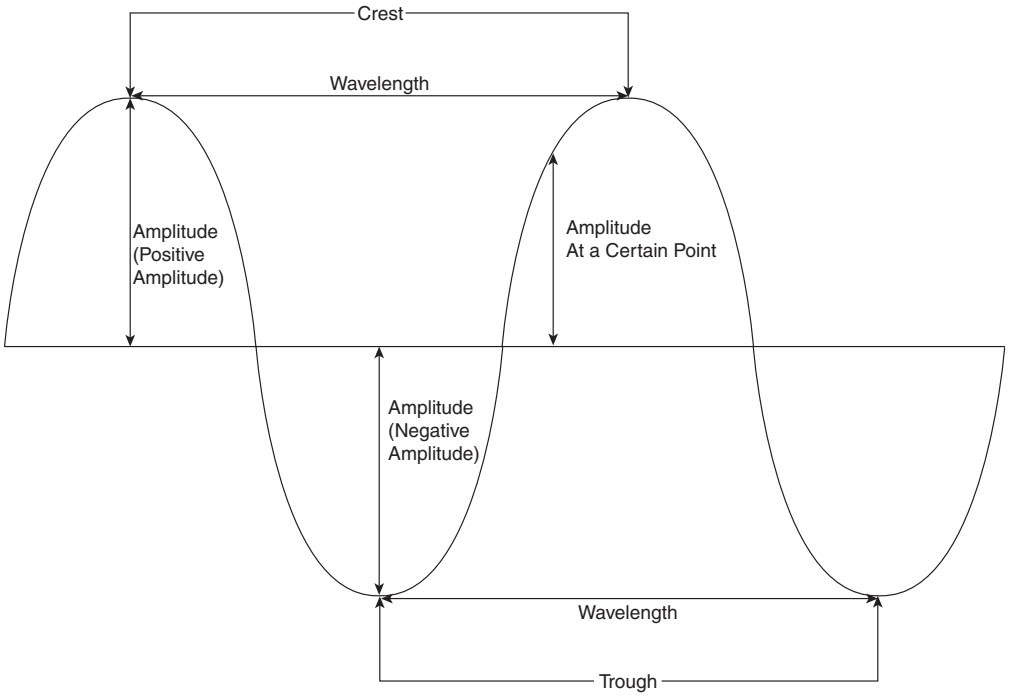

Figure 1-1 Different parts of a wave.

Radio or *radio frequency* (RF) waves are electromagnetic waves with wavelengths between 0.1 cm and 1,000 km. Another equivalent definition in terms of frequency is radio waves are electromagnetic waves whose frequencies lie between 30 Hz and 300 GHz. Other electromagnetic wave types are infrared, visible light wave, ultraviolet, gamma-ray, x-ray, and cosmic-ray.

RFID uses radio waves that are generally between the frequencies of 30 KHz and 5.8 GHz.

A *continuous wave* (CW) is a radio wave with constant frequency and amplitude. From a communications vantage, a CW does not have any embedded information in it but can be modulated to transmit a signal.

Modulation refers to the process of changing the characteristics of a radio wave to encode some information-bearing signal. Modulation can also refer to the result of applying the modulation process to a radio wave.

Radio waves can be affected by the material through which they propagate. A material is called *RF-lucent* or *RF-friendly* for a certain frequency if it lets radio waves at this frequency pass through it without any substantial loss of energy. A material is called *RF-opaque* if it blocks, reflects, and scatters RF waves. A material can allow the radio waves to propagate through it but with substantial loss of energy. These types of materials are referred to as *RF-absorbent*. The RF-absorbent or RF-opaque property of a material is *relative*, because it depends on the frequency. That is, a material that is RF-opaque at a certain frequency could be RF-lucent at a different frequency. The RF properties of some example materials are provided in Table 1-2, following a discussion of RFID frequency types.

Classes of RFID frequency types include the following:

- Low frequency (LF)
- High frequency (HF)
- Ultra high frequency (UHF)
- Microwave frequency

The following subsections discuss these frequency types.

1.1.1 Low Frequency (LF)

Frequencies between 30 KHz and 300 KHz are considered low, and RFID systems commonly use the 125 KHz to 134 KHz frequency range. A typical LF RFID system operates at 125 KHz or 134.2 KHz. RFID systems operating at LF generally use passive tags (discussed in Section 1.2.1), have low data-transfer rates from the tag to the reader, and are especially good if the operating environment contains metals, liquids, dirt, snow, or mud (a very important characteristic of LF systems). Active LF tags (discussed in Section 1.2.1) are also available from vendors. Because of the maturity of this type of tag, LF tag systems probably have the largest installed base. The LF range is accepted worldwide.

1.1.2 High Frequency (HF)

HF ranges from 3 MHz to 30 MHz, with 13.56 MHz being the typical frequency used for HF RFID systems. A typical HF RFID system uses passive tags, has a slow data-transfer rate from the tag to the reader, and offers fair performance in the presence of metals and liquids. HF systems are also widely used, especially in hospitals (where it does not interfere with the existing equipment). The HF frequency range is accepted worldwide.

The next frequency range is called *very high frequency* (VHF) and lies between 30 and 300 MHz. Unfortunately, none of the current RFID systems operate in this range. Therefore, this frequency type is not discussed any further.

1.1.3 Ultra High Frequency (UHF)

UHF ranges from 300 MHz to 1 GHz. A typical passive UHF RFID system operates at 915 MHz in the United States and at 868 MHz in Europe. A typical active UHF RFID system operates at 315 MHz and 433 MHz. A UHF system can therefore use both active and passive tags and has a fast data-transfer rate between the tag and the reader, but performs poorly in the presence of metals and liquids (*not* true, however, in the cases of low UHF frequencies such as 315 MHz and 433 MHz). UHF RFID systems have started being deployed widely because of the recent RFID mandates of several large private and public enterprises, such as several international and national retailers, the U.S. Department of Defense, and so on (see Chapter 10, "Standards"). The UHF range is *not* accepted worldwide.

1.1.4 Microwave Frequency

Microwave frequency ranges upward from 1 GHz. A typical microwave RFID system operates either at 2.45 GHz or 5.8 GHz, although the former is more common, can use both semi-active

and passive tags, has the fastest data-transfer rate between the tag and the reader, and performs very poorly in the presence of metals and liquids. Because antenna length is inversely proportional to the frequency (see Section 1.2.1.1.2), the antenna of a passive tag operating in the microwave range has the smallest length (which results in a small tag size because the tag microchip can also be made very small). The 2.4 GHz frequency range is called *Industry, Scientific, and Medical* (ISM) band and is accepted worldwide.

International restrictions apply to the frequencies that RFID can use. Therefore, some of the previously discussed frequencies might not be valid worldwide. Table 1-1 lists some example frequency-use restrictions for RFID together with the maximum allowable *power* and *duty cycle* (explained later in this chapter).

Table 1-1 International RFID Frequency Regulations

Country/ Region	LF	HF	UHF	Microwave
United States	125–134 KHz	13.56 MHz 10 watts effective radiated power (ERP)	902-928 MHz, 1 watt ERP or 4 watts ERP with a directional antenna with at least 50-channel hopping.	2400–2483.5 MHz, 4 watts, ERP 5725–5850 MHz, 4 watts ERP
Europe	125–134 KHz	13.56 MHz	865–865.5 MHz, 0.1 watts ERP, Listen Before Talk (LBT). 865.6–867.6 MHz, 2 watts ERP, LBT. 867.6–868 MHz, 0.5 watts ERP, LBT.	2.45 GHz
Japan	125–134 KHz	13.56 MHz	Not allowed. MPHPT (Ministry of Public Management, Home Affairs, Posts and Telecommunications) has opened up 950–956 MHz band for experimentation.	2.45 GHz
Singapore	125–134 KHz	13.56 MHz	923–925 MHz. 2 watts ERP.	2.45 GHz
China	125–134 KHz	13.56 MHz	Not allowed. Future possibility: 840–843 MHz and/or 917-925 MHz. SAC (Standardization Administration of China) is entrusted to formulate the RFID regulations.	2446–2454 MHz, 0.5 watts ERP

Table 1-2 lists RF properties of some example materials.

Table 1-2 RF Properties of Example Material Types

Material	LF	HF	UHF	Microwave
Clothing	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Dry wood	RF-lucent	RF-lucent	RF-lucent	RF-absorbent
Graphite	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Liquids (some types)	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Metals	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Motor oil	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Paper products	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Plastics (some types)	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Shampoo	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Water	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Wet wood	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent

Radio waves are susceptible to interference from various sources, such as the following:

- Weather conditions such as rain, snow, and other types of precipitation. However, as mentioned before, these are not an issue at LF and HF.
- The presence of other radio sources such as cell phones, mobile radios, and so on.
- Electrostatic discharge (ESD). ESD is a sudden flow of electrical current through a material that is an insulator under normal circumstances. If a large potential difference exists between the two points on the material, the atoms between these two points can become charged and conduct electric current.

The discussion now turns to how RFID technology works.

A radio device called a *tag* is attached to the object that needs to be identified. Unique identification data about this tagged object is stored on this tag. When such a tagged object is presented in front of a suitable RFID reader, the tag transmits this data to the reader (via the reader antenna). The reader then reads the data and has the capability to forward it over suitable communication channels, such as a network or a serial connection, to a software application running on a computer. This application can then use this unique data to identify the object presented to the reader. It can then perform a variety of actions such as updating the location information of this object in the database, sending an alert to the floor personnel, or completely ignoring it (if a duplicate read, for example).

As you can understand from this description, RFID is also a data-collection technology. However, this technology has some unique characteristics that enable users to apply it in areas beyond the reach of traditional data-collection technologies, such as bar codes.

An RFID application is implemented by an RFID system, which constitutes the entire technology end-to-end.

1.2 RFID System

An *RFID system* is an integrated collection of components that implement an RFID solution.

An RFID system consists of the following components (in singular form) from an *end-to-end* perspective:

- **Tag.** This is a mandatory component of any RFID system.
- **Reader.** This is a mandatory component, too.
- **Reader antenna.** This is another mandatory component. Some current readers available today have built-in antennas.
- **Controller.** This is a mandatory component. However, most of the new-generation readers have this component built in to them.
- **Sensor, actuator, and annunciator.** These optional components are needed for external input and output of the system.
- **Host and software system.** Theoretically, an RFID system can function independently without this component. Practically, an RFID system is close to worthless without this component.
- **Communication infrastructure.** This mandatory component is a collection of both wired and wireless network and serial connection infrastructure needed to connect the previously listed components together to effectively communicate with each other.

Figure 1-2 is a schematic diagram of an RFID system. Figure 1-3 shows an instantiation of this schematic with example components.

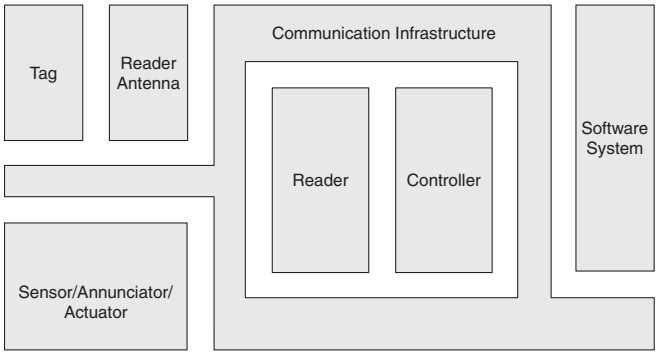

Figure 1-2 A schematic diagram of an RFID system.

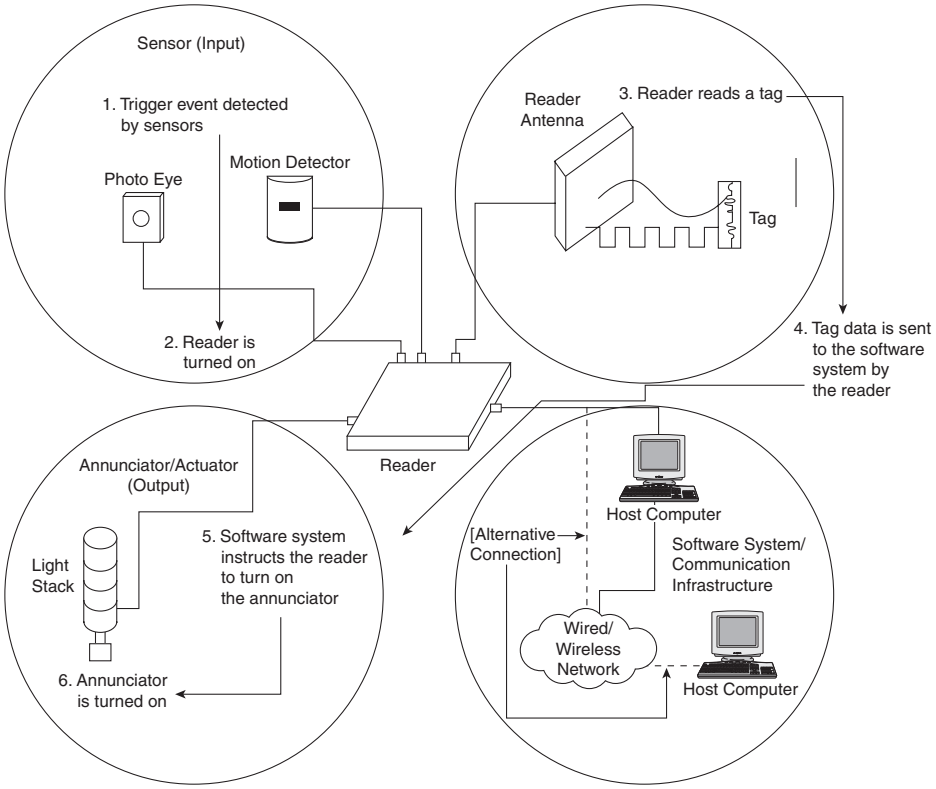

Figure 1-3 An RFID system with example components.

These figures may seem "reader-centric" because the RFID reader seems to be at the center of the entire system. Therefore, this figure might seem to be slanted, for example, toward the RFID vendor viewpoint. Figure 1-4 shows another perspective of the same system.

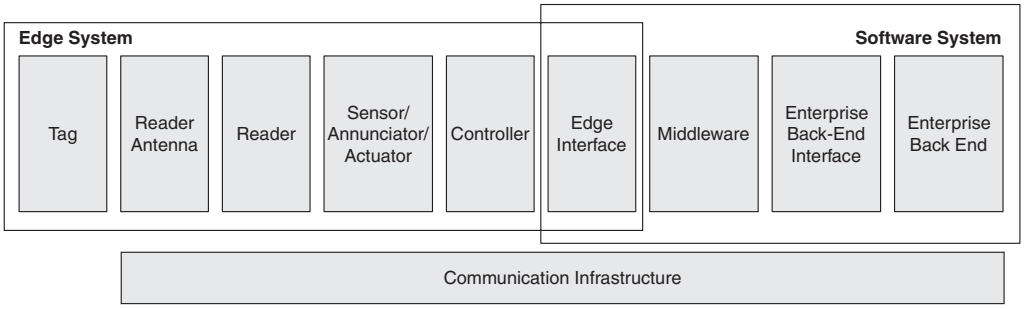

Figure 1-4 An RFID system from an IT perspective.

Note that in this scheme, the reader (together with the tag and antenna) is located at the *edge* of the system. This figure might be interpreted as how an RFID system looks from an IT or system-integrator perspective.

An RFID system thus has two parts—the first part (edge) governed by laws of physics and the second part involving information technology (IT). Which one is more important? The correct answer is "both." A state-of-the-art IT system is worthless if the data from its physical counterpart is unreliable and patchy. Similarly, a finely tuned RFID hardware setup is useless if the associated IT system cannot intelligently manage and process the data generated by this system.

An RFID system supports bidirectional communication flows, from the readers to the back end and from the back end to the readers (as also shown in Figure 1-3).

The following subsections discuss these previously identified RFID system components in detail.

1.2.1 Tag

An RFID *tag* is a device that can store and transmit data to a reader in a contactless manner using radio waves.

RFID tags can be classified in two different ways. The following list shows the first classification, which is based on whether the tag contains an on-board power supply and/or provides support for specialized tasks:

- Passive
- Active
- Semi-active (also known as semi-passive)

The following subsections discuss these in detail. (The other classification is discussed after this.)

1.2.1.1 Passive Tags

This type of RFID tag does not have an on-board power source (for example, a battery), and instead uses the power emitted from the reader to energize itself and transmit its stored data to the reader. A passive tag is simple in its construction and has no moving parts. As a result, such a tag has a long life and is generally resistant to harsh environmental conditions. For example, some passive tags can withstand corrosive chemicals such as acid, temperatures of 400ºF (204ºC approximately), and more.

In tag-to-reader communication for this type of tag, a reader always communicates first, followed by the tag. The presence of a reader is mandatory for such a tag to transmit its data.

A passive tag is typically smaller than an active or semi-active tag. It has a variety of read ranges starting with less than 1 inch to about 30 feet (9 meters approximately).

A passive tag is also generally cheaper compared to an active or semi-active tag.

A *contactless smart card* is a special type of passive RFID tag that is widely used today in various areas (for example, as ID badges in security and loyalty cards in retail). The data on this

card is read when it is in close proximity to a reader. The card does not need to be physically in contact with the reader for reading.

A passive tag consists of the following main components:

- Microchip
- Antenna

Figure 1-5 shows the components of a passive tag.

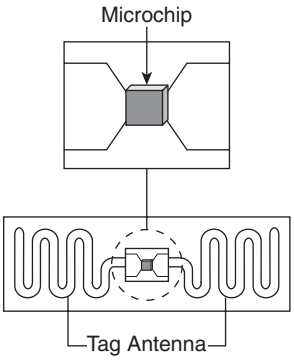

Figure 1-5 Components of a passive tag.

The following subsections discuss these components in detail.

1.2.1.1.1 Microchip

Figure 1-6 shows the basic components of a microchip.

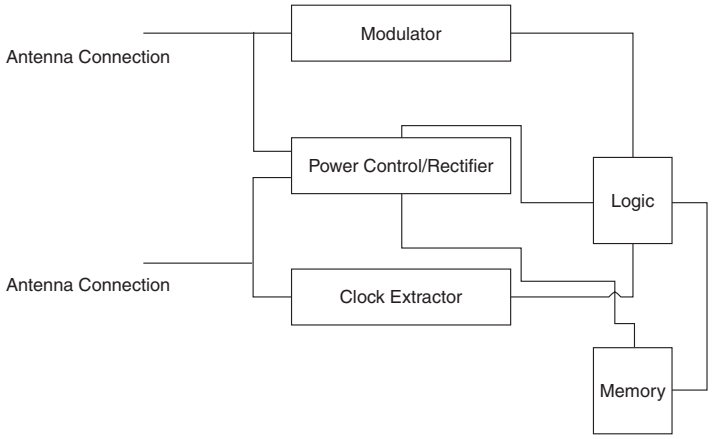

Figure 1-6 Basic components of a microchip.

The *power control/rectifier* converts AC power from the reader antenna signal to DC power. It supplies power to the other components of the microchip. The *clock extractor* extracts the clock signal from reader antenna signal. The *modulator* modulates the received reader signal. The tag's response is embedded in the modulated signal, which is then transmitted back to the reader. The *logic* unit is responsible for implementing the communication protocol between the tag and the reader. The microchip *memory* is used for storing data. This memory is generally segmented (that is, consists of several blocks or fields). *Addressability* means the ability to address (that is, read or write) the individual memory of a tag's microchip. A tag memory block can hold different data types, such as a portion of the tagged object identifier data, checksum (for example, cyclic redundancy check [CRC]) bits for checking the accuracy of the transmitted data, and so on. Recent advances in technology have shrunk the size of the microchip to less than the size of a grain of sand. However, a tag's physical dimensions are not determined by the size of its microchip but by the length of its antenna.

1.2.1.1.2 Antennas

A tag's antenna is used for drawing energy from the reader's signal to energize the tag and for sending and receiving data from the reader. This antenna is physically attached to the microchip. The antenna geometry is central to the tag's operations. Infinite variations of antenna designs are possible, especially for UHF, and designing an effective antenna for a tag is as much as an art as a science. The antenna length is directly proportional to the tag's operating wavelength. A *dipole* antenna consists of a straight electric conductor (for example, copper) that is interrupted at the center. The total length of a dipole antenna is half the wavelength of the used frequency to optimize the energy transfer from the reader antenna signal to the tag. A *dual dipole* antenna consists of two dipoles, which can greatly reduce the tag's alignment sensitivity. As a result, a reader can read this tag at different tag orientations. A *folded dipole* consists of two or more straight electric conductors connected in parallel and each half the wavelength (of the used frequency) long. When two conductors are involved, the resulting folded dipole is called *2-wire folded dipole*. A *3-wire folded dipole* consists of three conductors connected in parallel. Figure 1-7 shows these antenna types.

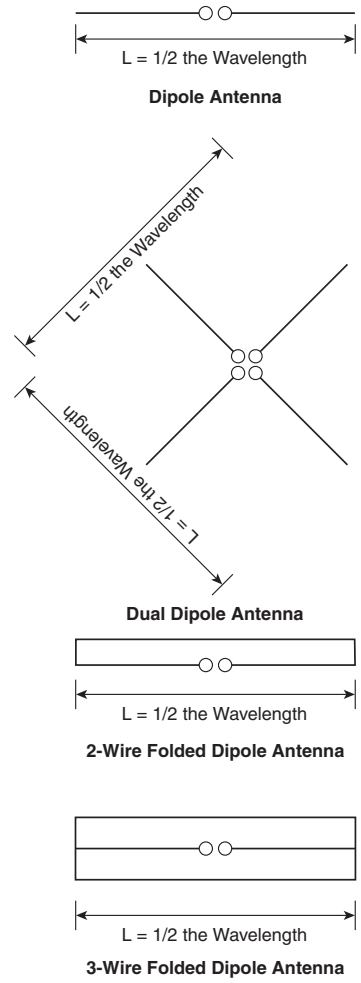

Figure 1-7 Dipole antenna types.

A tag's antenna length is generally much larger than the tag's microchip, and therefore ultimately determines a tag's physical dimensions. An antenna can be designed based on several factors, such as the following:

- Reading distance of the tag from the reader
- Known orientation of the tag to the reader
- Arbitrary orientation of the tag to the reader
- Particular product type(s)
- Speed of the tagged object
- Specific operating condition(s)
- Reader antenna polarization

The connection points between a tag's microchip and the antenna are the weakest links of the tag. If any of these connection points are damaged, the tag might become nonfunctional or might have its performance significantly degraded. An antenna designed for a specific task (such as tagging a case) might perform poorly for a different task (such as tagging an individual item in the case). Changing antenna geometry randomly (just "hacking around;" for example, cutting or folding it) is not a good idea because this can detune the tag, resulting in suboptimal performance. However, someone who knows what he is doing can deliberately modify a tag's antenna to detune it (drilling a hole into it, for example) and actually increase the readability of the tag!

Currently, a tag antenna is constructed with a thin strip of a metal (for example, copper, silver, or aluminum). In the future, however, it will be possible to print antennas directly on the tag label, case, and product packaging using a conductive ink that contains copper, carbon, or nickel. Effort is also currently underway to determine whether the microchip might be printed with such an ink, too. These future enhancements may enable you to print an RFID tag just as you do a bar code on the case and item packaging. As a result, the cost of an RFID tag might drop substantially below the anticipated $.05 per tag. Even without the ability to print a microchip, a printed antenna can be attached to a microchip to create a complete RFID tag much faster than attaching a metal antenna.

Figures 1-8 through 1-10 show passive tags from various vendors.

Figure 1-8 Family of LF tags from Texas Instruments.

Reprinted with permission from Texas Instruments

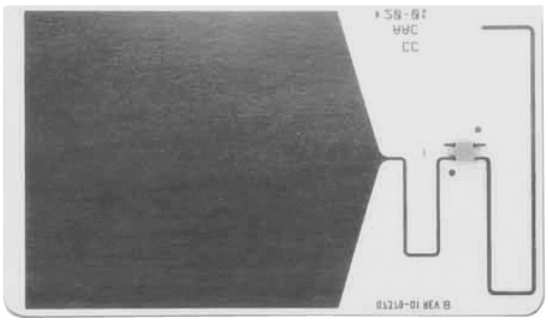

Figure 1-9 915 MHz tag from Intermec Corporation.

Reprinted with permission from Intermec Technologies Corporation

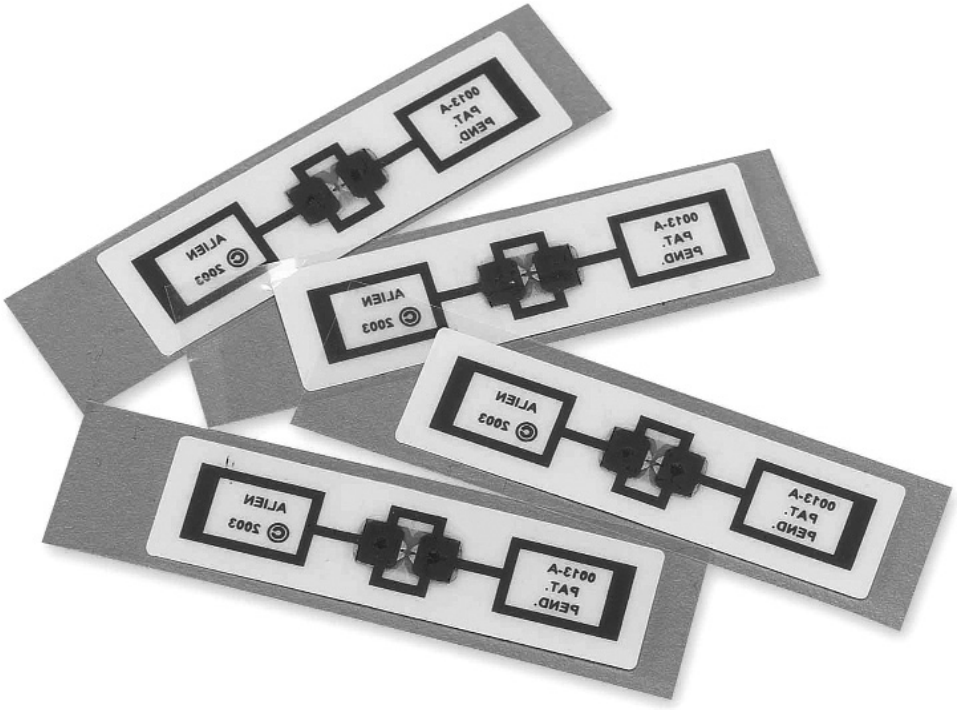

Figure 1-10 2.45 GHz tags from Alien Technology.

Reprinted with permission from Alien Technology

1.2.1.2 Active Tags

Active RFID tags have an on-board power source (for example, a battery; other sources of power, such as solar, are also possible) and electronics for performing specialized tasks. An active tag uses its on-board power supply to transmit its data to a reader. It does not need the reader's emitted power for data transmission. The on-board electronics can contain microprocessors, sensors, and input/output ports powered by the on-board power source. Therefore, for example, these components can measure the surrounding temperature and generate the average temperature data. The components can then use this data to determine other parameters such as the expiry date of the attached item. The tag can then transmit this information to a reader (along with its unique identifier). You can think of an active tag as a wireless computer with additional properties (for example, like that of a sensor or a set of sensors).

In tag-to-reader communication for this type of tag, a tag always communicates first, followed by the reader. Because the presence of a reader is not necessary for data transmission, an active tag can broadcast its data to its surroundings even in the absence of a reader. This type of active tag, which continuously transmits data with or without the presence of a reader, is also called a *transmitter*. Another type of active tag enters a sleep or a low-power state in the absence of interrogation by a reader. A reader wakes up such a tag from its sleep state by issuing an appropriate command. This state saves the battery power, and therefore, a tag of this type generally has a longer life compared to an active transmitter tag. In addition, because the tag transmits only when interrogated, the amount of induced RF noise in its environment is reduced. This type of active tag is called a *transmitter/receiver* (or a *transponder*). As you can understand from this discussion, you cannot accurately call all tags transponders.

The reading distance of an active tag can be 100 feet (30.5 meters approximately) or more when the active transmitter of such a tag is used.

An active tag consists of the following main components:

- **Microchip.** The microprocessor size and capabilities are generally greater than the microchips found in passive tags.
- **Antenna.** This can be in the form of an RF module that can transmit the tag's signals and receive reader's signals in response. For a semi-active tag, this is composed of thin strip(s) of metal such as copper, similar to that of a passive tag.
- **On-board power supply.**
- **On-board electronics.**

Figure 1-11 shows examples of active and semi-active tags.

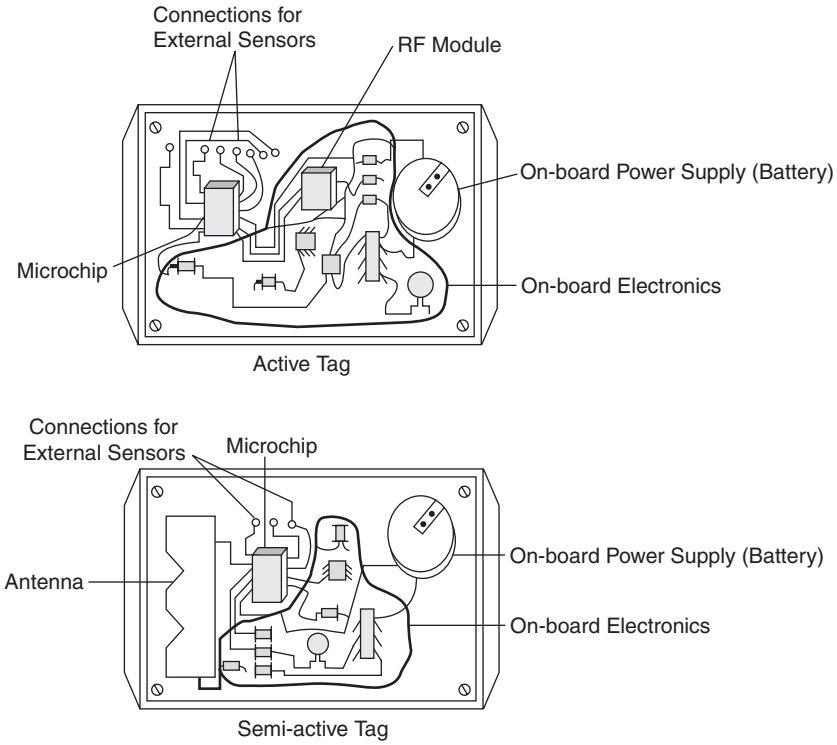

Figure 1-11 Example active and semi-active tags.

The first two components have already been described in the previous section. The last two components are discussed now.

1.2.1.2.1 On-Board Power Supply

All active tags carry an on-board power supply (for example, a battery) to provide power to its on-board electronics and to transmit data. If a battery is used, an active tag generally lasts for about 2 to 7 years depending on the battery life. One of the determining factors of the battery life is the data-transmission rate interval of the tag—the larger the interval, the longer the battery and hence the tag life. For example, suppose that an active tag is made to transmit once every few seconds. If you increase this so that the tag transmits once every few minutes or even once every few hours, you extend the battery life. The on-board sensors and processors consume power and can shorten the battery life, too.

When the battery of an active tag is completely discharged, the tag stops transmitting messages. A reader that was reading these messages does not know whether the tag's battery has died or whether the tagged product has disappeared from its read zone unless the tag transmits its battery status to this reader.

1.2.1.2.2 On-Board Electronics

The on-board electronics allow the tag to act as a transmitter, and optionally allow it to perform specialized tasks such as computing, displaying the values of certain dynamic parameters, acting as a sensor, and so on. This component can also provide an option for connecting external sensors. Therefore, depending on the sensor type attached, such a tag can perform a wide variety of sensing tasks. In other words, the range of functionality of this component is virtually limitless. Note that as the functionality and hence the physical size of this component grows, the tag might grow in size. This growth is acceptable because no hard limit applies to the size of an active tag as long as it can be deployed (that is, properly attached to the object that needs to be tagged). This means active tags can be applied to a wide range of applications, several of which might not even exist today.

1.2.1.3 Semi-Active (Semi-Passive) Tags

Semi-active tags have an on-board power source (for example, a battery) and electronics for performing specialized tasks. The on-board power supply provides energy to the tag for its operation. However, for transmitting its data, a semi-active tag uses the reader's emitted power. A semi-active tag is also called a *battery-assisted tag*. In tag-to-reader communication for this type of tag, a reader always communicates first, followed by the tag. Why use a semi-passive tag over a passive tag? Because a semi-active tag does not use the reader's signal, unlike a passive tag, to excite itself, it can be read from a longer distance as compared to a passive tag. Because no time is needed for energizing a semi-active tag, such a tag could be in the read zone of a reader for substantially less time for its proper reading (unlike a passive tag). Therefore, even if the tagged object is moving at a high speed, its tag data can still be read if a semi-active tag is used. Finally, a semi-active tag might offer better readability for tagging of RF-opaque and RF-absorbent materials. The presence of these materials might prevent a passive tag from being properly excited, resulting in failure to transmit its data. However, this is not an issue with a semi-active tag.

The reading distance of a semi-active tag can be 100 feet (30.5 meters approximately) under ideal conditions using a modulated backscatter scheme (in UHF and microwave).

Figures 1-12 through 1-14 show active and semi-active tags from various vendors.

Figure 1-12 Mantis low UHF (303.8 MHz) active tag with built-in motion detector from RFCode, Inc.

Reprinted with permission from RFCode, Inc.

Figure 1-13 915 MHz/2.45 GHz semi-active tags from TransCore.

Reprinted with permission from TransCore

Figure 1-14 2.45 GHz semi-active tags from Alien Technology.

Reprinted with permission from Alien Technology

The next classification, as shown here, is based on the capability to support data rewrites:

- Read-only (RO)
- Write once, read many (WORM)
- Read-write (RW)

Both active and passive tags can be RO, WORM, and RW. The following sections discuss these classifications in detail.

1.2.1.4 Read Only (RO)

An RO tag can be programmed (that is, written) just once in its lifetime. The data can be burned into the tag at the factory during the manufacturing stage. To accomplish this, the individual fuses on the tag microchip are burned permanently using a fine-pointed laser beam. After this is done, the data cannot be rewritten for the entire lifetime of the tag. Such a tag is also called *factory programmed*. The tag manufacturer supplies the data on the tag, and the tag users typically do not have any control over it. This type of tag is good for small applications only, but is impractical for large manufacturing or when tag data needs to be customized based on the application. This tag type is used today in small pilots and business applications.

1.2.1.5 Write Once, Read Many (WORM)

A WORM tag can be programmed or written once, which is generally done not by the manufacturer but by the tag user right at the time when the tag needs to be created. In practice, however, because of buggy implementation, it is possible to overwrite particular types of WORM tag data several times (about 100 times is not uncommon)! If the data for such a tag is rewritten more than a certain number of times, the tag can be damaged permanently. A WORM tag is also called *field programmable*.

This type of tag offers a good price-to-performance ratio with reasonable data security, and is the most prevalent type of tag used in business today.

1.2.1.6 Read Write (RW)

An RW tag can be reprogrammed or rewritten a large number of times. Typically, this number varies between 10,000 and 100,000 times and above! This rewritability offers a tremendous advantage because the data can be written either by the readers or by the tag itself (in case of active tags). An RW tag typically contains a Flash or a FRAM memory device to store its data. An RW tag is also called *field programmable* or *reprogrammable*. Data security is a challenge for RW tags. In addition, this type of tag is most expensive to produce. RW tags are not widely used in today's applications, a fact that might change in the future as the tag technology and applicability increases with a decrease in tag cost.

It is important to briefly pause here and describe a type of RFID tag called *surface acoustic wave* (SAW) before moving on to the next topic.

1.2.1.7 SAW (Surface Acoustic Wave) Tags

A SAW tag differs fundamentally from microchip-based tags. SAW tags have started appearing on the market, and might be widely used in the future. Currently, SAW devices are widely used in cell phones, color televisions, and so on.

SAW tags use low-power RF waves in the ISM 2.45 GHz frequency range for their operation. Unlike a microchip-based tag, a SAW tag does not need DC power to energize itself for data transmission. Figure 1-15 shows how such a tag operates.

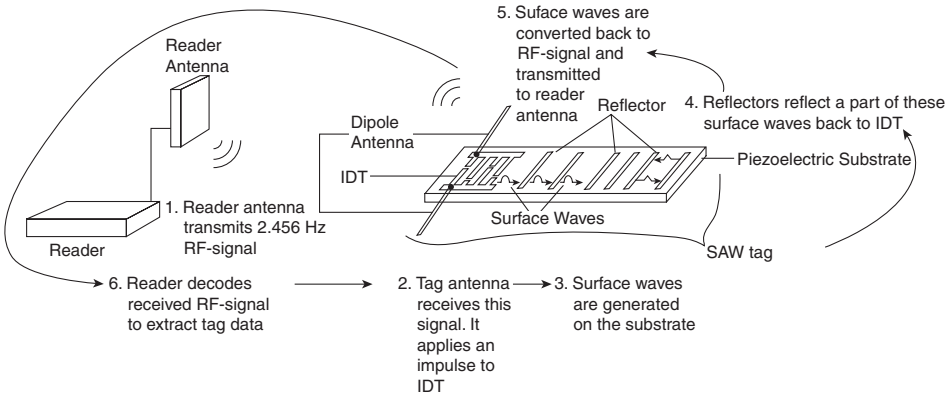

Figure 1-15 SAW tag operation.

A SAW tag consist of a dipole antenna attached to an *interdigital transducer* (IDT) placed on a piezoelectric substrate made of lithium niobate or lithium tantalate. A series of well-placed individual electrodes acting as reflectors (made of aluminum or etched on the substrate) are positioned on the substrate. The antenna applies an electrical impulse to the IDT when it receives the RF signal from a SAW reader. This impulse generates surface waves, also known as *Raleigh* waves, typically traveling at 3,000 to 4,000 meters per second on the substrate. Some of these waves are reflected back to the IDT by the reflectors; the rest are absorbed by the substrate. The reflected waves form a unique pattern, determined by the reflector positions, representing the tag data. These waves are converted back to the RF signal in the IDT and transmitted back to the RFID reader via the tag antenna. The reader then decodes the received signal to extract the tag data.

The advantages of a SAW tag include the following:

- Uses very low power because it does not need a DC source of power to energize itself.
- Can successfully tag RF-opaque and RF-absorbent materials, such as metal and water, respectively.
- Has a longer read range compared to a microchip tag operating in the same frequency range (that is, 2.45 GHz).
- Can operate with short bursts of RF-signal in contrast to microchip-based tags, which need much longer signal duration from reader to the tag.
- Has high read accuracy rates.
- Is hardy because of its simple design.
- Does not need anti-collision protocols. Anti-collision protocols need to be implemented at the reader level only instead of at both reader and tag level as for a microchip tag (thus reducing the cost of a SAW tag).

SAW readers are less prone to interference with other SAW readers. SAW tags might very well be the only choice in certain tagging situations and are likely to be widely used in the future.

Some tags can transmit data to a reader without using RF waves. A brief description of such tags follows.

1.2.1.8 Non-RFID Tags

The concept of attaching a tag and having it wirelessly transmit its unique ID to a reader is not the exclusive domain of RF waves. You can use other types of wireless communications for this purpose. For example, you can use ultrasonic and infrared waves for tag-to-reader communication.

Ultrasonic communication has the additional advantages that it does not cause interference with existing electrical equipment and cannot penetrate through walls. As a result, ultrasonic tagging systems can be deployed in hospitals, where such technology can coexist with the existing medical equipment. In addition, an ultrasonic reader and a tag must be within the same room for

the tag to be read by the reader. This required proximity can prove helpful in asset monitoring and tracking.

An infrared tag uses light to transmit its data to a reader. Because light cannot penetrate through walls, an infrared tag and reader must both be in the same room for communication. If an obstacle covers the light source of a tag, the tag can no longer communicate with a reader (a serious disadvantage).

1.2.2 Readers

An RFID reader, also called an *interrogator*, is a device that can read from and write data to compatible RFID tags. Thus, a reader also doubles up as a writer. The act of writing the tag data by a reader is called *creating* a tag. The process of creating a tag and uniquely associating it with an object is called *commissioning the tag*. Similarly, *decommissioning a tag* means to disassociate the tag from a tagged object and optionally destroy it. The time during which a reader can emit RF energy to read tags is called the duty cycle of the reader. International legal limits apply to reader duty cycles.

The reader is the central nervous system of the entire RFID hardware system—establishing communication with and control of this component is the most important task of any entity which seeks integration with this hardware entity.

A reader has the following main components:

- Transmitter
- Receiver
- Microprocessor
- Memory
- Input/output channels for external sensors, actuators, and annunciators (Although, strictly speaking, these are optional components, they are almost always provided with a commercial reader.)
- Controller (which may reside as an external component)
- Communication interface
- Power

Figure 1-16 shows an example reader with these components.

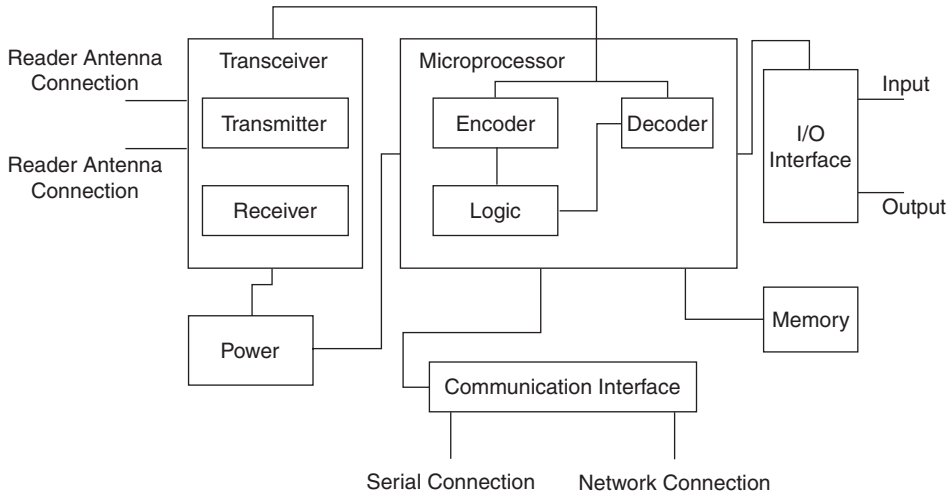

Figure 1-16 The components of an example reader.

The following subsections describe these components.

1.2.2.1 Transmitter

The reader's transmitter is used to transmit AC power and the clock cycle via its antennas to the tags in its read zone. This is a part of the *transceiver* unit, the component responsible for sending the reader's signal to the surrounding environment and receiving tag responses back via the reader antenna(s). The antenna ports of a reader are connected to its *transceiver* component. One reader antenna can be attached to each such antenna port. Currently, some readers can support up to four antenna ports.

1.2.2.2 Receiver

This component is also part of the *transceiver* module. It receives analog signals from the tag via the reader antenna. It then sends these signals to the reader microprocessor, where it is converted to its equivalent digital form (that is, the digital representation of the data that the tag has transmitted to the reader antenna).

1.2.2.3 Microprocessor

This component is responsible for implementing the reader protocol to communicate with compatible tags. It is performs decoding and error checking of the analog signal from the receiver. In addition, the microprocessor might contain custom logic for doing low-level filtering and processing of read tag data.

1.2.2.4 Memory

Memory is used for storing data such as the reader configuration parameters and a list of tag reads. Therefore, if the connection between the reader and the controller/software system goes down, not all read tag data will be lost. Depending on the memory size, however, a limit applies as to how many such tag reads can be stored at any one time. If the connection remains down for an extended period with the reader reading tags during this downtime, this limit might be exceeded and part of the stored data lost (that is, overwritten by the other tags that are read later).

1.2.2.5 Input/Output Channels for External Sensors, Actuators, and Annunciators

Readers do not have to be turned on for reading tags at all times. After all, the tags might appear only at certain times in the read zone, and leaving readers perpetually on would just waste the reader's energy. In addition, as mentioned previously, regulatory limits apply to the reader duty cycle, too. This component provides a mechanism for turning a reader on and off depending on external events. A sensor of some sort, such as a motion or light sensor, detects the presence of tagged objects in the reader's read zone. This sensor can then set the reader on to read this tag. Similarly, this component also allows the reader to provide local output depending on some condition via an annunciator (for example, sounding an audible alarm) or an actuator (for example, opening or closing a security gate, moving a robot arm, and so forth). Sensors, actuators, and annunciators are discussed later in this chapter.

1.2.2.6 Controller

A *controller* is an entity that allows an external entity, either a human or a computer program, to communicate with and control a reader's functions and to control annunciators and actuators associated with this reader. Often, manufacturers integrate this component into the reader itself (as firmware, for example). However, it is also possible to package this as a separate hardware/software component that must be bought together with the reader. Controllers are discussed in detail later in this chapter.

1.2.2.7 Communication Interface

The communication interface component provides the communication instructions to a reader that allow it to interact with external entities, via a controller, to transfer its stored data and to accept commands and send back the corresponding responses. You can assume that this interface component is either part of the controller or is the medium that lies between a controller and the external entities. This entity has important characteristics that make it necessary to treat this as an independent component. A reader could have a serial as well as a network interface for communication. A serial interface is probably the most widespread type of reader interface available, but next-generation readers are being developed with network interfaces as a standard feature. Sophisticated readers offer features such as automatic discovery by an application, embedded Web servers that allow the reader to accept commands and display the results using a standard Web browser, and so forth.

1.2.2.8 Power

This component supplies power to the reader components. The power source is generally provided to this component through a power cord connected to an appropriate external electrical outlet.

Like tags, readers can also be classified using two different criteria. The first criterion is the interface that a reader provides for communication. Based on this, readers can be classified as follows:

- Serial
- Network

The following subsections describe these reader types.

1.2.2.9 Serial Reader

Serial readers use a serial communication link to communicate with an application. The reader is physically connected to a computer's serial port using an RS-232 or RS-485 serial connection. Both of these connections have an upper limit on the cable length that can be used to connect a reader to a computer. RS-485 allows a longer cable length than RS-232 does.

The advantage of serial readers is that the communication link is reliable compared to network readers. Therefore, the use of these readers is recommended to minimize dependency on a communication channel.

The disadvantage of serial readers is the dependence on the maximum length of cable that can be used to connect a reader to a computer. In addition, because the number of serial ports is generally limited on a host, a larger number of hosts (as compared to the number of hosts needed for network readers) might be needed to connect to all the serial readers. Another problem is maintenance—if the firmware needs to be updated, for example, maintenance personnel might have to physically deal with each reader. Also, the serial data-transmission rate is generally lower than the network data-transmission rate. These factors might result in higher maintenance costs and significant operation downtime.

1.2.2.10 Network Reader

Network readers can be connected to a computer using both wired and wireless networks. In effect, the reader behaves like a network device installation that does not require any specialized knowledge of the hardware. Note, however, that SNMP-type monitoring features are currently available for just a few network reader types. Therefore, the majority of these readers cannot be monitored as standard network devices.

The advantage of network readers is that there is no dependence on the maximum length of cable that can be used to connect a reader to a computer. A smaller number of hosts are generally needed as compared to the serial readers. In addition, the reader firmware can be updated remotely over the network without any need to visit the reader physically. This can ease the maintenance effort and lower the cost of ownership of such an RFID system.

The disadvantage of network readers is that the communication link is not as reliable compared to serial readers. When the communication link goes down, the back end cannot be

accessed. As a result, the RFID system might come to a complete standstill. The readers, in general, have internal memory to store tag reads. This feature might somewhat alleviate short network outages.

The next classification of reader type can be made based on its mobility, as follows:

- Stationary
- Handheld

The following subsections describe these reader types.

1.2.2.11 Stationary Reader

A stationary reader, also called a *fixed* reader, is what its name implies. These readers are mounted on a wall, portal, or some suitable structure in the read zone. The structure on which the reader is mounted may not be static! For example, some stationary readers are mounted on forklifts. Similarly, you can mount these readers inside delivery trucks. In contrast to tags, readers are not generally very tolerant of harsh environmental conditions. Therefore, if you install a reader outdoors or on moving objects, take care to ruggedize it properly. Stationary readers generally need external antennas for reading tags. A reader can provide up to four external antennas ports.

The cost of a stationary reader is generally less than the cost of handheld readers. Stationary readers are the most common type of reader used today.

Figures 1-17 and 1-18 show some fixed readers.

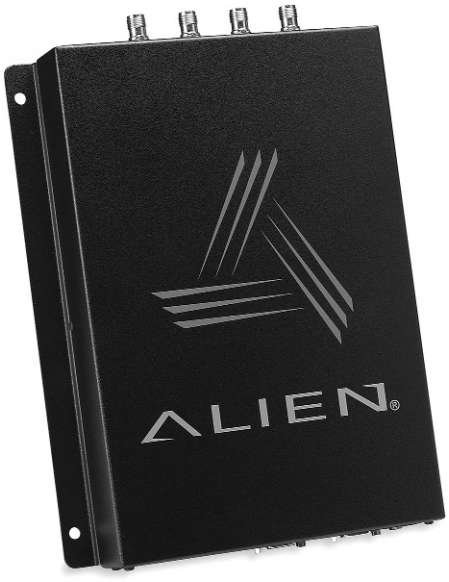

Figure 1-17 UHF fixed network reader from Alien Technology.

Reprinted with permission from Alien Tecnology

Figure 1-18 Low UHF (303.8 MHz) fixed wired/wireless (802.11b) network reader from RFCode, Inc.

Reprinted with permission from RFCode, Inc.

A type of reader called an *agile reader* can operate in different frequencies or can use different tag-to-reader communications protocols. Today's agile readers are generally stationary.

A type of stationary reader called an *RFID printer* can print a bar code and create (that is, write) an RFID tag on a *smart label* in an integrated operation. A smart label consists of a bar code label that has an embedded RFID tag in it. Various types of information, such as the sender and recipient addresses, product information, and free-form text, can be printed on the label, too. An RFID printer reads the smart label tag that it has just written to validate the write operation. If this validation fails, the printer rejects the smart label that it has just printed. This device obviates the necessity to separately create an RFID tag where bar codes are currently used (which might reduce additional logistics overhead). A business that is using bar codes today for its operations can use RFID printers as a first step in adopting the RFID technology. The bar code information provides a human-readable identification of the tagged object. Also, the existing systems and operations can keep using the same bar code data with some or no change. The notes area of the label can provide the embedded tag ID in human-readable form. The RFID tag can provide object-level Auto-ID capabilities and other associated benefits. Figure 1-19 shows an example smart label. Figure 1-20 shows an example RFID printer.

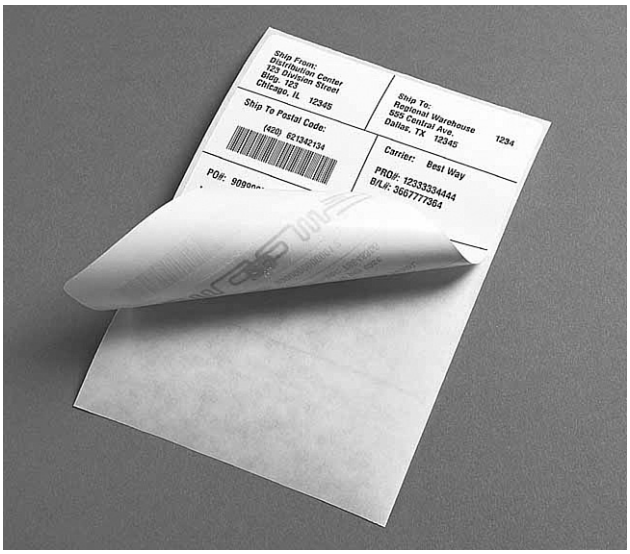

Figure 1-19 RFID smart label from Zebra Technologies.

Reprinted with permission from Zebra Technologies

Figure 1-20 RFID printer from Zebra Technologies.

Reprinted with permission from Zebra Technologies

A stationary reader can generally operate in the following modes:

- Autonomous
- Interactive

The following subsections describe these modes.

1.2.2.11.1 Autonomous Mode

In autonomous mode, a reader continuously read tags in its read zone. Every time a tag is read, it is saved to a list, usually called a *tag list*. An item on the tag list is associated with what is generally called a *persist time*. If the associated tag cannot be read for a period of time exceeding its persist time, it is dropped from the tag list. An application running on a host machine can register itself to receive the tag list periodically. A tag list includes information such as the following:

- Unique tag identifiers
- Reading time
- How many times a particular tag has been read since it has been discovered (that is, first read by the reader)
- The antenna ID that read a particular tag
- Reader name

1.2.2.11.2 Interactive Mode

In interactive mode, a read receives and executes commands from an application running on a host machine or from a user using a vendor-supplied client to communicate with the reader. After the reader fully executes the current command, it waits for the next. A reader can execute a range of commands, from sending the current tag list to the command invoker to changing the reader's configuration parameters.

1.2.2.12 Handheld Reader

A handheld reader is a mobile reader that a user can operate as a handheld unit. A handheld reader generally has built-in antenna(s). Although these readers are typically the most expensive (and few are commercially available), recent advances in reader technology are resulting in sophisticated handheld readers at lower prices. Figures 1-21 shows a handheld reader.

Figure 1-21 UHF handheld reader from Intermec Corporation.

Reprinted with permission from Intermec Technologies Corporation

The following section introduces the underlying communication mechanisms between a tag and a reader.

1.2.2.13 Communication Between a Reader and a Tag

Depending on the tag type, the communication between a reader and a tag can be one of the following:

- Modulated backscatter
- Transmitter type
- Transponder type

Before delving into the details of these communication types, it is important for you to understand the concepts of near field and far field.

The area between a reader antenna and one full wavelength of the RF wave emitted by the antenna is called *near field*. The area beyond one full wavelength of the RF wave emitted from a reader antenna is called *far field*. Passive RFID systems operating in LF and HF use near field communication, whereas those in UHF and microwave frequencies use far field communication. The signal strength in near field communication attenuates as the cube of the distance from the reader antenna. In far field, it attenuates as square of the distance from the reader antenna. As a

result, far field communication is associated with a longer read range compared with near field communication.

Next, a comparison between tag read and tag write is in order.

Tag write takes a longer time than tag read under the same conditions because a write operation consists of multiple additional steps, including an initial verification, erasing any existing tag data, writing the new tag data, and a final verification phase. In addition, the data is written on the tag in blocks in multiple steps. As a result, a single tag write can take hundreds of milliseconds to complete and increases with the increase in data size. In contrast, several tags can be read in this time interval by the same reader. Also, tag write is a sensitive process that needs the target tag to be closer (compared to its corresponding read distance) to the reader antenna for the entire write operation. This closer proximity ensures the tag antenna can derive sufficient energy from the reader antenna signal to power its microchip so that it can execute the write instructions. The power requirement for write operation is generally significantly higher than that required for reading. The write operation might fail otherwise. However, a tag does not have to stay close to the reader during a read operation. Also, during tag write operation, any tag other than the target should not be in write range of the reader. Otherwise, in some cases, this other tag might accidentally get written rather than the target tag. This write range issue is clearly not relevant during a read operation, when multiple tags can exist in the read range of the reader at the same time.

1.2.2.13.1 Modulated Backscatter

Modulated backscatter communication applies to passive as well as to semi-active tags. In this type of communication, the reader sends out a *continuous wave* (CW) RF signal containing AC power and clock signal to the tag at the *carrier frequency* (the frequency at which the reader operates). Through physical coupling (that is, a mechanism by which the transfer of energy takes place from the reader to the tag), the tag antenna supplies power to the microchip. The word excite is frequently used to indicate a passive tag microchip drawing power from a reader's signal to properly energize itself. About 1.2 volts are generally necessary to energize the tag microchip for reading purposes. For writing, the microchip usually needs to draw about 2.2 volts from the reader signal. The microchip now modulates or breaks up the input signal into a sequence of on and off patterns that represents its data and transmits it back. When the reader receives this modulated signal, it decodes the pattern and obtains the tag data.

Thus, in modulated backscatter communication, the reader always "talks" first, followed by the tag. A tag using this scheme cannot communicate at all in the absence of a reader because it depends totally on the reader's power to transmit its data. Figure 1-22 shows backscatter communication.

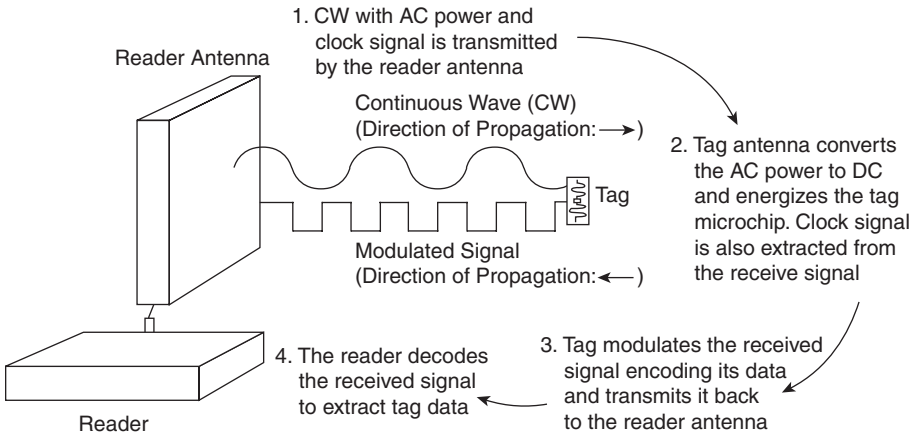

Figure 1-22 Backscatter communication.

A related term, *beam power*, is also used in this context, and means that a tag is using the reader's power to modulate the reader signal back. Note that a passive tag exclusively uses beam power to transmit its data. A semi-active tag uses beam power to clock its oscillator and generate the transmit signal back. Thus, in essence, a semi-active tag also uses beam power to transmit its data.

1.2.2.13.2 Transmitter Type

This type of communication applies to active tags only. In this type of communication, the tag broadcasts its message to the environment in regular intervals, irrespective of the presence or absence of a reader. Therefore, in this type of communication, the tag always "talks" first rather than the reader. Figure 1-23 shows transmitter communication.

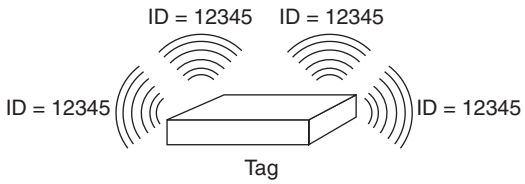

Figure 1-23 Transmitter communication.

1.2.2.13.3 Transponder Type

This type of communication applies to a special type of active tags called transponders (as discussed previously). In this type of communication, the tag goes to a "sleep" or into a dormant stage in the absence of interrogation from a reader. In this state, the tag might periodically send a message to check whether any reader is listening to it. When a reader receives such a query message, it can instruct the tag to "wake up" or end the dormant state. When the tag receives this

command from the reader, it exits its current state and starts to act as a transmitter tag again. (That is, it starts broadcasting its message periodically to its surroundings.) In this type of communication, the tag data is sent only when the reader specifically asks for it. Figure 1-24 shows transponder communication.

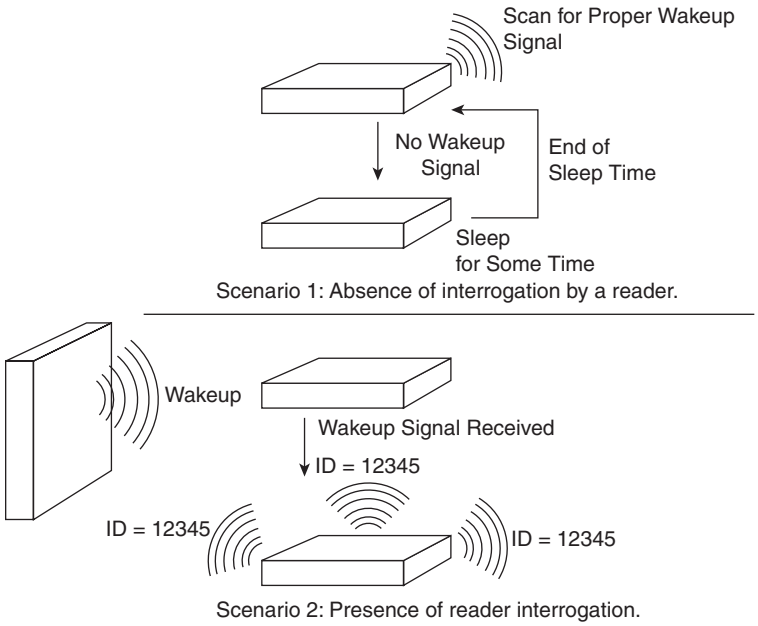

Figure 1-24 Transponder communication.

1.2.3 Reader Antenna

A reader communicates to a tag through the reader's antennas, a separate device that is physically attached to a reader, at one of its antenna ports, by means of a cable. This cable length is generally limited to between 6 and 25 feet. (However, this length limit may vary.) As mentioned previously, a single reader can support up to four antennas (that is, have four physical antenna ports). A reader antenna is also called the reader's *coupling element* because it creates an electromagnetic field to *couple* with the tag. An antenna broadcasts the reader transmitter's RF signal into its surroundings and receives tag responses on the reader's behalf. Therefore, proper positioning of the antennas, *not the readers*, is essential for good read accuracy (although a reader has to be located somewhat close to an antenna because of the limitation of the antenna cable length). In addition, some stationary readers might have in-built antennas. As a result, in this case, positioning the antennas for a reader is equivalent to positioning the reader itself. In general, RFID reader antennas are shaped like rectangular or square boxes. Figures 1-25 and 1-26 show some reader antennas.

Figure 1-25 UHF Circular polarized reader antenna from Alien Technology.

Reprinted with permission from Alien Technology

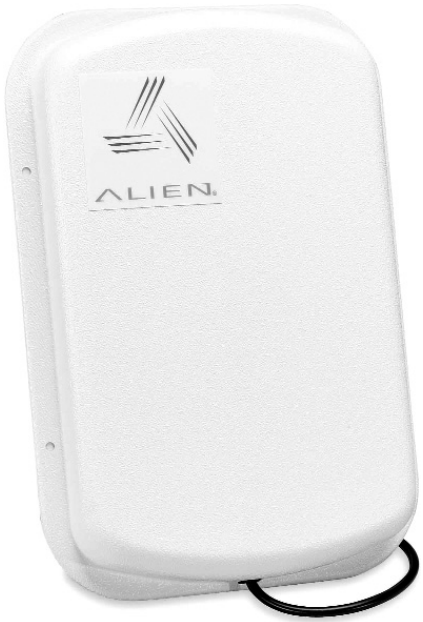

Figure 1-26 UHF Linear polarized reader antenna from Alien Technology.

Reprinted with permission from Alien Technology

It is now time to discuss a very important concept of an antenna: the antenna footprint.

1.2.3.1 Antenna Footprint

The footprints of the reader's antennas determine the read zone (also called the *read window*) of a reader. In general, an antenna footprint, also called an *antenna pattern*, is a three-dimensional region shaped somewhat like an ellipsoid or a balloon projecting out of the front of the antenna. In this region, the antenna's energy is most effective; therefore, a reader can read a tag placed inside this region with the least difficulty. Figure 1-27 shows such a simple antenna pattern.

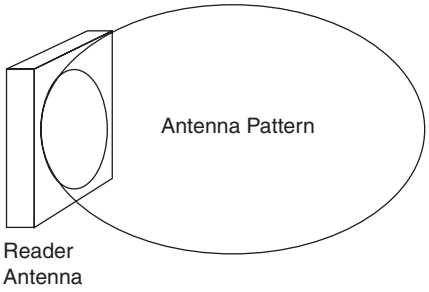

Figure 1-27 Simple antenna pattern.

In reality, because of antenna characteristics, the footprint of an antenna is never uniformly shaped like an ellipsoid but almost always contains deformities or protrusions. Each protrusion is surrounded by dead zones. Such dead zones are also called *nulls*. Figure 1-28 shows an example of such an antenna pattern.

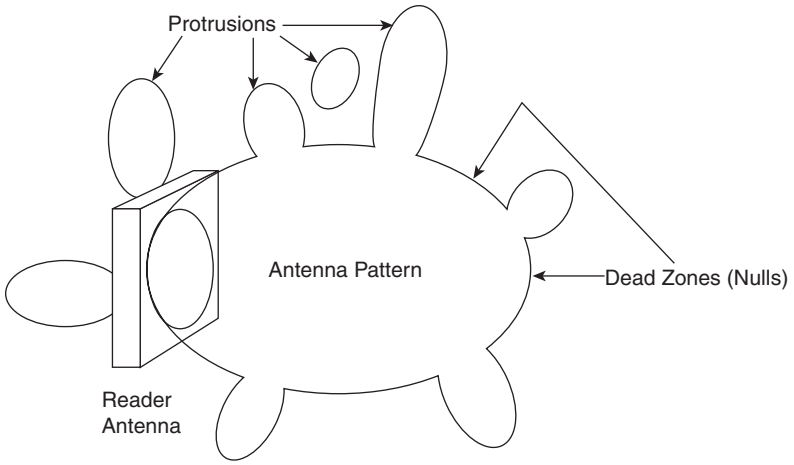

Figure 1-28 An example antenna pattern containing protrusions.

The reflection of reader antenna signals on RF-opaque objects causes what is known as *multipath*. In this case, the reflected RF waves are scattered and can arrive at the reader antenna at different times using different paths. Some of the arriving waves could be *in phase* (that is, exactly match with the original antenna signal's wave pattern). In this case, the original antenna signal is enhanced when these waves impose with the original waves giving rise to protrusions. This phenomenon is also known as *constructive interference*. Some of the waves could also arrive out of phase (that is, the exact opposite of the original antenna wave pattern). In this case, the original antenna signal is cancelled when these two wave types impose on each other. This is also called *destructive interference*. Nulls are created as a result. Figure 1-29 shows an example of multipath.

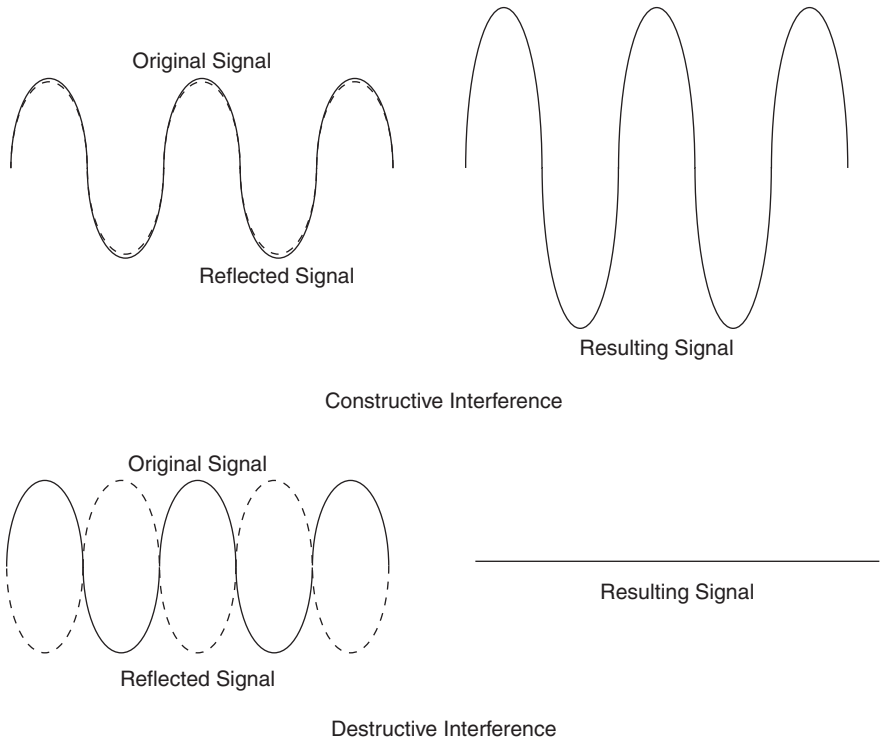

Figure 1-29 A multipath schematic.

A tag placed in one of the protruded regions will read, but if this tag moves slightly so that it is inside the surrounding dead region, the tag cannot be read (which might lead to nonintuitive tag-reading behavior). For example, when placed a certain distance away from a reader, a tag does not read, but when moved slightly in one direction, it can be read by the reader; if this tag is then moved slightly in another direction, however, it cannot be read! The read behavior of a tag near a protruded region is thus unreliable. Therefore, when you place an antenna to cover a read

area, it is important that you *not* depend on these protruded regions to maximize the read distance. The best strategy is to stay inside the main ellipsoid-shaped region even if it means sacrificing the read range by a few feet—better safe than sorry.

It is extremely important to determine the antenna footprint; the antenna footprint determines where a tag can or cannot be read. The manufacturer might provide the antenna footprint as part of the antenna's specifications. However, you should use such information as a guideline only, because the actual footprint will most likely vary depending on the operating environment. You can use well-defined techniques such as *signal analysis* to map an antenna footprint. In signal analysis, the signal from the tag is measured, using equipment such as a *spectrum analyzer* and/or a *network analyzer*, under various conditions (for example, in free space, different tag orientations, and on conductive materials or absorptive materials). By analyzing these signal strengths, you can precisely determine the antenna footprint.

Antenna polarization, another important concept of reader antenna design, is discussed in the following section.

1.2.3.2 Antenna Polarization

As discussed previously, an antenna emits electromagnetic waves into its surroundings. The direction of oscillation of these electromagnetic waves is called the *polarization* of the antenna. What does this mean to tag readability? A great deal! The readability of a tag, together with its reading distance and reading robustness, greatly depends on the antenna polarization and the angle at which the tag is presented to the reader.

The main antenna types in UHF, based on polarization, are

- Linear polarized
- Circular polarized

The following subsections discuss these two types of antennas.

1.2.3.2.1 Linear Polarized Antenna

In this antenna type, the RF waves emanate in a linear patter from the antenna. These waves have only one energy field. Figure 1-30 shows the resulting wave pattern emanating from a linear polarized antenna.

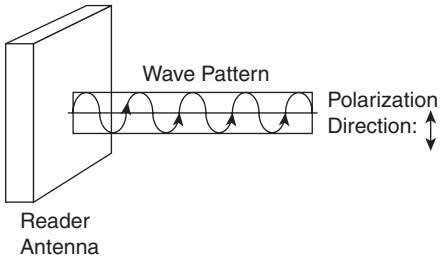

Figure 1-30 Wave pattern from a linear polarized antenna.

A linear polarized antenna has a narrower radiation beam with a longer read range compared to a circular polarized antenna. In addition, a narrower radiation beam helps a linear polarized antenna to read tags within a longer, narrow but well-defined read region (compared to a circular polarized antenna), instead of reading tags randomly from its surroundings. However, a linear polarized antenna is sensitive to tag orientation with respect to its polarization direction. These types of antenna are therefore useful in applications where the tag orientation is fixed and predictable. Figure 1-31 shows how a tag should be oriented with respect to a linear antenna for its proper reading in case of backscatter communication.

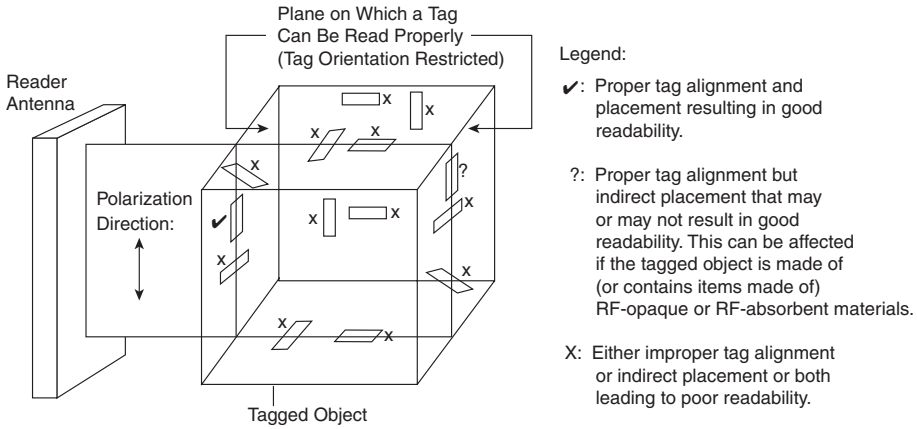

Figure 1-31 Proper tag orientation for a linear polarized antenna.

1.2.3.2.2 Circular Polarized Antenna

RF waves radiate from a circular polarized antenna in a circular pattern. These waves have two constituting energy fields that are equal in amplitude and magnitude, but have a phase difference of 90º. Therefore, when a wave of an energy field is at its highest value, the wave of the other field is at its lowest. Figure 1-32 shows the resulting wave pattern emanating from a circular polarized antenna.

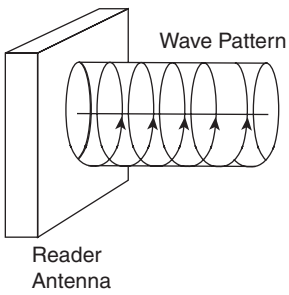

Figure 1-32 Wave pattern from a circular polarized antenna.

Because of the nature of polarization, a circular polarized antenna is largely unaffected by tag orientation. Therefore, this type of antenna proves ideal for applications where the tag orientation is unpredictable. A circular polarized antenna has a wider radiation beam and hence reads tags in a wider area compared to a linear polarized antenna. This antenna is preferred for an RFID system that uses high UHF or microwave frequencies in an operating environment where there is a high degree of RF reflectance (due to presence of metals and so forth). Figure 1-33 shows how a tag should be oriented with respect to a circular antenna for its proper reading in case of backscatter communication.

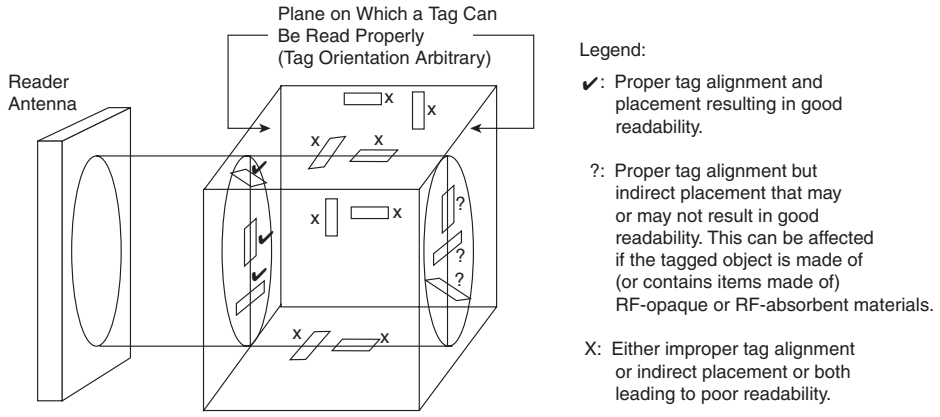

Figure 1-33 Proper tag orientation for a circular polarized antenna.

Figure 1-34 shows the circular and linear polarized antenna patterns.

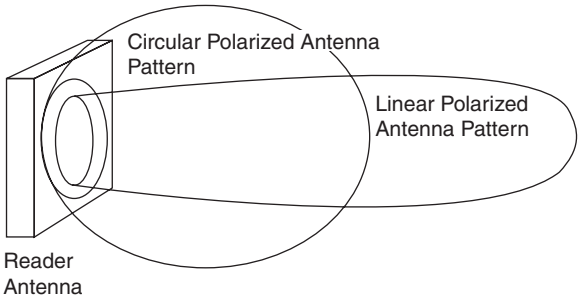

Figure 1-34 Circular and linear polarized antenna patterns.

Often, a *patch* antenna is used for making UHF antennas, as described in the following subsection.

1.2.3.2.3 Patch Antenna

A patch antenna, also called a *microstrip* or *planar antenna*, in its basic form consists of a rectangular metal foil or a plate mounted on a substrate such as Teflon. The other side of the substrate is coated with a metallic substance. A microstrip connected to the rectangular metal foil supplies power to the antenna (see Figure 1-35). The power supply type can be varied to make a patch antenna circular or linear polarized.

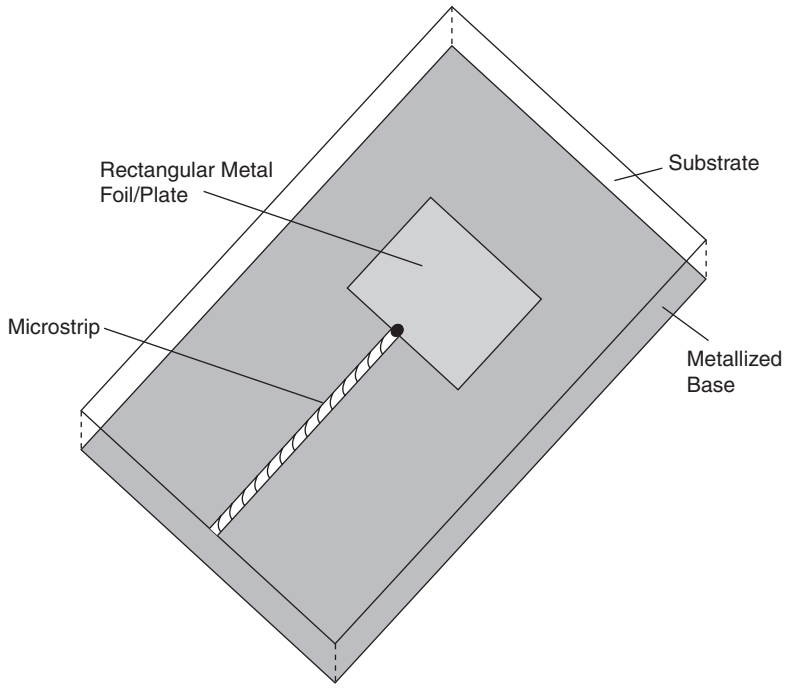

Figure 1-35 An basic patch antenna.

1.2.3.3 Antenna Power

An antenna emits power measured in either *effective radiated power* (ERP) units in Europe or in *equivalent isotropic radiated power* (EIRP) units in the United States. ERP and EIRP are not the same but are related by the relation EIRP = 1.64 ERP. The maximum possible value of antenna power is limited by national and international (for example, FCC in the United States) regulations. To use an antenna with higher power than the allowable limit, you must obtain explicit permission from the appropriate regulatory body. You can always reduce antenna power, however, by placing a small device called an *attenuator* in the transmission line (for example, between an antenna connector and the reader port). As a result, the antenna's signal strength is reduced, and the antenna's read range is diminished. Attenuation proves very useful in situations where the read zone needs to be constrained as a part of system requirements so that tags are only read

inside but not outside this region. The ability of an attenuator to reduce the antenna strength varies depending on the attenuator.

1.2.4 Controller

A *controller* is an intermediary agent that allows an external entity to communicate with and control a reader's behavior together with the annunciators and actuators associated with this reader. A controller is the *only* component of an RFID system (or a reader, depending on point of view) through which reader communications are possible; no other medium or entity provides this ability. As mentioned previously, a controller for a reader can be embedded inside the reader or can be a separate component by itself. An analogy is in order. A controller to a reader is what a printer driver is for a computer printer. To print a document from a computer to a printer, the computer must have the appropriate printer driver software installed. Similarly, to retrieve tag data stored on a reader, a computer must use a controller—it cannot communicate to the reader in any other way.

A controller also provides (or uses, depending on viewpoint) a communication interface for the external entities to interact with it (as described previously in the section about readers).

1.2.5 Sensor, Annunciator, and Actuator

A reader does not have to be turned all the time; it can be started (and stopped) automatically if needed. A sensor can be attached with a reader for this purpose. This sensor can then be used to turn on/off the reader based on some external event detected by this sensor. A sensor can thus be used to provide some kind of input trigger to a reader.

An *annunciator* is an electronic signal or indicator. Examples of annunciators include audible alarms, strobes, light stacks, and so on. A light stack consists of a vertical arrangement of different-colored indicators and is useful for displaying various statuses of different system attributes. For example, the red indicator might mean invalid or bad tag data in the read zone, green might indicate a valid tag read, and amber might signal network connection between the reader and the controller is down. Figures 1-36 shows an example light stack.

An *actuator* is a mechanical device for controlling or moving objects. Examples of actuators include a *programmable logic controller* (PLC), robot arm, mechanical arm for an access gate, and so on. A PLC is one of the most versatile actuators, and PLCs are widely used in manufacturing plants. PLCs enable a variety of actions to be performed (such as monitoring and controlling a product packaging line, or applying a predetermined amount of torque to nuts in a mechanical assembly [for example, an automobile]).

Annunciators and actuators can thus be used to provide some kind of local output from an RFID system, such as audio-visual alarms in case of a read failure, opening an access gate for a successful read, and so forth.

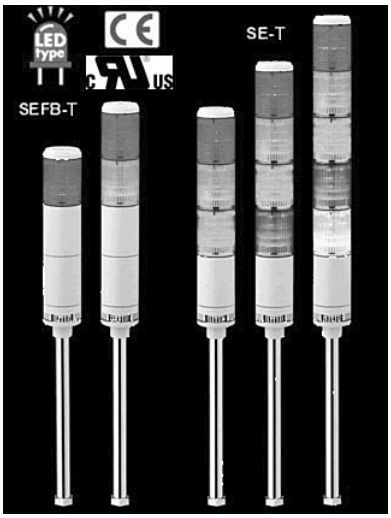

Figure 1-36 LED Signal Tower from Patlite Corporation.

Reprinted with permission from Patlite Corporation

1.2.6 Host and Software System

The *host and software system* is an all-encompassing term for the hardware and software component that is separate from the RFID hardware (that is, reader, tag, and antenna); the system is composed of the following four main components:

- Edge interface/system
- Middleware
- Enterprise back-end interface
- Enterprise back end

In a nontrivial RFID system, all these components are present to some degree. The following sections discuss these components.

1.2.6.1 Edge Interface/System

This component integrates the entire host and software system with the RFID hardware (which consists of the reader, tag, and antenna). This integration is accomplished by establishing communication with and control of the central nervous system of RFID hardware: the readers. Therefore, this component's main task is to get data from the readers, control the readers' behavior and use the readers to activate the associated external actuators and annunciators.

This component is logically and physically closest to the RFID hardware and can be considered to be at the edge when viewed from the host and software system perspective. Therefore, this is also the right place for this component to activate external actuators and annunciators

without any need to go through the reader. This placement proves very useful because then the choice and control capabilities of annunciators and actuators are not limited by the reader support, but can be extended as and when needed by customizing the *edge system*.

The edge system is also the perfect place to hide the nitty-gritty details of interaction with a specific reader (through its controller) from a particular manufacturer. Therefore, this component also provides an abstraction layer for any type of readers needed by the RFID system. This abstraction layer is very desirable because then the rest of the host and software system can use this abstraction to interact with any supported readers, present and future, without any need to change itself.

This component can be viewed as a kind of a super controller that can be used to interact with any supported reader controller in the RFID system.

Moreover, this component can do several other tasks that are beyond the responsibilities of a simple controller, such as the following:

- Filter out duplicate reads from different readers
- Allow setting of event-based triggers that can automatically activate an annunciator or an actuator
- Provide intelligent functions such as aggregating and selectively sending out tag data to host and software system
- Remote reader management
- Remote management of itself

As apparent from the preceding discussion, this component may actually be hosted on specialized hardware as an embedded system. The rest of the host and software system can then interact with this embedded system over a wired or a wireless network. This component can be implemented using a standard such as *Open Services Gateway initiative* (OSGi), which defines a standard for dynamic delivery of software services to network devices (see Chapter 10). In a very simple case of a trivial, possibly throwaway, pilot, this component might be completely absent.

1.2.6.2 Middleware

The *middleware* component can be broadly defined as everything that lies between the edge interface and the enterprise back-end interface. This component can be viewed as the central nervous system of the RFID system from the software perspective (RFID readers can be considered the same from an RFID hardware perspective) in that it provides core functionality of the system, including the following:

- Data sharing both inside and outside of an enterprise
- Efficient management of massive data produced by RFID system
- Provide generic components that can be used as building blocks for implementing the business specific filtering and aggregation logic

- Open standard based so that it is compatible with a wide range of other software systems
- Enable loose coupling between the edge interface and the enterprise back-end interface (and thus any change in the former will minimally affect the latter)

In the extreme case of a trivial, possibly throwaway, pilot, this component might be completely absent.

This is the most complex and important component of the host and software system. As a result, a principle part of the implementation effort will be spent on implementing this component. Therefore, when implementing an RFID system, it is always preferable to procure this component as an off-the-shelf system from RFID software and services vendors. You can then customize it to meet the application requirements.

1.2.6.3 Enterprise Back-End Interface

The *enterprise back-end interface* component is used to integrate the middleware component with the enterprise back-end component. This is the place for implementing business process integration. Which processes need to be integrated with the RFID system will determine the amount of effort needed to implement this component. This effort can be substantial if business process changes are involved or comprehensive.

Because the middleware is a generic component, some customization is almost always needed to trigger transactions and transfer data between it and the enterprise back end. It is not uncommon to find enterprise-scale integration interfaces natively built in to the enterprise scale systems, such as ERP and WMS, that are available from large third-party software vendors.

1.2.6.4 Enterprise Back End

The enterprise back-end component encompasses the complete suite of applications and IT systems of an enterprise. This is thus the data repository and the business processes engine for the entire enterprise. In an RFID system context, this component provides the directory data for the tagged objects to the middleware component.

Note that in general, integration with a handful of applications or systems is necessary to achieve a satisfactory integration with the enterprise back end and hence the business processes. This is, of course, assuming that this component is well architected and implemented.

This component generally involves minimum effort from the implementation perspective of an RFID system because this is already built and functional. However, in some cases (for example, proprietary system elements), some effort might be necessary to actually modify or enhance this component to make it compatible with the RFID system that is being built.

1.2.7 Communication Infrastructure

This component provides connectivity and enables security and systems management functionalities for different components of an RFID system, and is therefore an integral part of the system. It includes the wired and wireless network, and serial connections between readers, controllers, and computers. The wireless network type can range from a *personal area network* (PAN,

provided by Bluetooth), to a *local area network* (LAN, offered by 802.11x technology), to a *wide area network* (WAN, provided by 2.5G/3G technologies). Satellite communication networks, for example, using geosynchronous L-band satellites are also becoming an increasing reality for RFID systems that need to work in a very wide geographical area where existence of a pervasive reader infrastructure is not guaranteed.

It is now time to pause for a moment and learn about the basic concepts of an RFID system.

1.2.8 Basic Concepts

This section discusses the following terms that are frequently used in reference to an RFID system:

- Frequency
- Tag collision
- Reader collision
- Tag readability
- Read robustness

Frequency is the *most important* attribute of an RFID system. It has already been discussed in detail in the beginning of this chapter.

The remaining terms are discussed in detail now in the following subsections.

1.2.8.1 Tag Collision

Contrary to popular belief, a reader can only communicate with one tag at a time. When more than one tag attempts to communicate with the reader at the same time, a *tag collision* is said to occur. In this case, in response to the reader's query, multiple tags reflect back their signals at the same time to the reader, confusing it. A reader then needs to communicate with the conflicting tags using what is called a *singulation protocol*. The algorithm that is used to mediate tag collisions is called an *anti-collision algorithm*. Currently, the following two types of anti-collision algorithms are most widely used:

- ALOHA for HF
- Tree Walking for UHF

Using one of these anti-collision algorithms, a reader can identify several tags in its read zone in a very short period of time. Thus, it appears that this reader is communicating with these tags almost simultaneously.

1.2.8.2 Reader Collision

When the read zone (or read window) of two or more readers overlap, the signal from one reader can interfere with the signal from another. This phenomenon is called *reader collision*. This situation can arise if the antennas of these two readers are installed in such a manner that it gives rise to *destructive interference* (antenna footprint). As a result, RF energy from one of the antennas of

a reader "cancels out" the RF energy from one of the antennas of the other reader. To avoid this problem, position the reader antennas so that the antenna of one reader does not directly face the antenna of another reader. If the direct facing of these antennas is unavoidable, separate them a sufficient distance so that their read zones do not overlap. You can use proper attenuators to attune the antenna power to achieve this. In addition, two antennas of the same reader can generally overlap without creating a reader collision, because the power to the antennas is physically transferred by the reader in such a manner that only one antenna is active at a time. As a result, there is no chance of two or more antennas of this reader emitting signals at the same time. You can also use another technique, called *time division multiple access* (TDMA), to avoid reader collision. In this scheme, the readers are instructed to read at different times rather than all reading at the same time. As a result, the antenna of only one reader is active at a time. The problem with this approach is that a tag can be read more than one time by different readers in the overlapping read zone. Therefore, some intelligent filtering mechanism must be implemented by the controller or the edge system/interface to filter out the duplicate tag reads.

1.2.8.3 Tag Readability

Tag readability of an RFID system for a particular operating environment can be defined as the capability of the system to read a specific tag data successfully. Tag readability depends on a number of factors (see Chapter 9, "Designing and Implementing an RFID Solution"). From a simple perspective, an RFID system needs to read a tag successfully just once to provide good tag readability. To make this guarantee, however, the system should be designed so that it can read a single tag several times, so that even if a tag read fails several times there's a good chance that one of the reads will succeed. In other words, an RFID system should have good read for robustness. This is the topic of the next section.

1.2.8.4 Read Robustness

Read robustness (also called *read redundancy*) is the number of times a particular tag can be read successfully when inside a read zone. As noted in the previous section, an RFID system has to be designed such that it has good read robustness for the tags. The speed of a tagged object can negatively impact the read robustness as the amount of time spent by the tag in the read zone decreases with an increase in its speed. This results in a decrease of read robustness for this tag. The number of tags present at one time in the read zone also can hamper read robustness because the number of tags that can be read by a reader per unit time is limited.

1.2.9 Characterization of an RFID System

An RFID system can be characterized in three different ways using the following attributes:

- Operating frequency
- Read range
- Physical coupling method

These criteria are interrelated. The first two criteria are most frequently used in practice. All three characterizations are discussed next.

1.2.9.1 Characterization Based on Operating Frequency

Operating frequency is the most important attribute of an RFID system. It is the frequency at which the reader transmits its signal. It is closely associated with the typical reading distance attribute. In most cases, the frequency of an RFID system is determined by its typical reading distance requirement. Frequency has already been described earlier in this chapter.

1.2.9.2 Characterization Based on Read Range

Read range of an RFID system is defined as the reading distance between the tag and the reader. Using this criterion, an RFID system can be divided into the following three types:

- Close coupled
- Remote coupled
- Long range

The following subsections describe these types.

1.2.9.2.1 Close-Coupled System

The read range of the RFID systems belonging to this class is less than 1 cm. The LF and HF RFID systems belong to this category.

1.2.9.2.2 Remote-Coupled System

The RFID systems belonging to this class have a read range of 1 cm to 100 cm. Again, this category contains LF and HF RFID systems.

1.2.9.2.3 Long-Range System

RFID systems having a read range of more than 100 cm belong to this class. RFID systems operating in the UHF and microwave frequency range belong to this group.

1.2.9.3 Characterization Based on Physical Coupling Method

Physical coupling refers to the method used for coupling the tag and the antenna (that is, the mechanism by which energy is transferred to the tag from the antenna). Based on this criterion, three different types of RFID systems are possible:

- Magnetic
- Electric
- Electromagnetic

These following subsections discuss these different types.

1.2.9.3.1 Magnetic-Coupled System

These types of RFID systems are also known as *inductive-coupled systems* or *inductive-radio systems*. The LF and HF RFID systems belong to this category.

1.2.9.3.2 Electric-Coupled System

These types of RFID systems are also known as *capacitive-coupled systems*. The LF and HF RFID systems belong to this category.

1.2.9.3.3 Electromagnetic-Coupled System

The majority of RFID systems belonging to this class are also called *backscatter systems*. RFID systems operating in the UHF and microwave frequency range belong to this group.

1.3 Conclusion

This chapter provided an in-depth discussion of the RFID basics. Admittedly, it covered a plethora of information that might be difficult to assimilate in a single reading. However, a good knowledge of this material is crucial to understanding the technology and applying it to solve real-world challenges. The material in this chapter is used throughout this book to develop related concepts. The reader is advised to revisit this chapter several times until confident of a good grasp of the fundamentals. If you want to dive deeper into the theoretical aspects of RFID technology, consult the *RFID Handbook*, Second Edition, by Klaus Finkenzeller (John Wiley & Sons, 2003).