A

RFID Applied

1

The Stage Is Set

At some point in your life, you probably have used one of those credit-card-style security badges to gain entrance to a building, or driven past a toll road on one of those nonstop, boothless lanes. If so, you have experienced RFID applied.

1.1 What Is RFID?

In the simplest form, and as its name implies, radio frequency identification, or RFID, is the process and physical infrastructure by which a unique identifier, within a predefined protocol definition, is transferred from a device to a reader via radio frequency waves. It has taken many years of development to come up with a functional system, but the basic principle is not much different than that of the well-known barcode: Encode an identifier number in a machine-readable form that can be accessed quickly and reliably, with no human translation. However, it is not fair to say that RFID is just a glorified barcode transferred via radio frequency waves. The very nature of RFID, the fact that it is based on a microprocessor containing a data memory space, allows RFID chips to be applied in many instances that could not have been ever imagined with barcodes.

Imagine a world where a company has no problem finding inventory in a warehouse, or ensuring that the products it ships concur with the shipping order, or determining that the products received are all in the shipment, or avoiding stock-outs on the sales floor, or knowing the current stage of production of a particular product, or simply finding assets on its premises. This is the promise of RFID—a technology that can enable these situations to happen. If this is your idea of a perfect world, this book is for you, the business practitioner who needs to learn and understand how RFID can improve your business from a practical perspective.

The stage is set for RFID. In fact, it has been set for a while. People have been using RFID technology for many years, and mostly without noticing it. Everyday use of RFID technology has become common. It is so common, in fact, that until recently, many industries didn't even really think about its potential. It was a forgotten technology that had just a few, ubiquitous applications. Many businesses thought that the technology was either not robust enough for enterprise-wide deployment or not cost-effective enough to generate positive *returns on investments* (ROIs) in those deployments. The point of this book is to present a case of why this technology is important and how we see it changing the future of industry by supporting huge increases in automation, productivity, effectiveness, and cost-saving opportunities, eventually positively affecting the holy grail of the business world: a prosperous bottom line.

1.2 RFID Systems in the Real World

Before we get deep into the components that make up an RFID infrastructure, it will help to relate some examples of real-life implementation of RFID systems. As mentioned, RFID has been around for quite a while and there are many RFID applications that are used on a daily basis. Five of these are shown in the following paragraphs. Part B and Appendix A of this book go into greater detail about some of these, as well as other examples.

1.2.1 Toll Roads

This is probably one of the most common RFID applications used by millions of people on a daily basis. Many toll roads offer the option of a fast lane in which the driver does not have to stop at the toll booth to pay. Instead, the driver attaches a small device to (usually) the windshield that allows the driver to proceed through the fast lane at a reasonable speed (usually the speed limit). This small device, an *RFID tag*, is read by a *reader,* installed in the fast lane, as the car passes by (these terms are defined in the next section). The *reader* sends a signal to an *RFID-enabled system* with the unique identifier of the tag as well as other pertinent information such as date and time. This RFID-enabled system then uses a *database* to associate the tag identifier with the proper automobile and ultimately with the bill code associated with that automobile.

1.2.2 Newborn-Infant Tracking

Many hospitals have faced the erroneous swap of newborns with parents, creating great emotional distress for the parents as well as major legal liabilities. Some innovative hospitals started looking for a way to identify babies and to properly match them with their parents. RFID provides a great mechanism to ensure that the right baby is put in the arms of the right mother. Both the baby and the mother are affixed with a secure wristband that carries an RFID tag. The tag's unique identities are electronically associated with the baby and the mother at the time that the wristbands are put on (usually a few minutes after birth). From that moment until discharge time, the RFID wristbands are checked to ensure that the right baby is with the right mother.

1.2.3 High-Value Asset Tracking and Management

Although tracking every asset with RFID within, say, a warehouse, may be too daunting a task given today's technology, it may be very feasible to just track selected high-value items where the ROI of the RFID infrastructure makes sense. That is exactly what some companies are doing today. A good example of this is the recent move of some aerospace companies to start tagging high-valued engine components and tracking them not only within the manufacturing plants and warehouses but also in the field. The U.S. Navy has run pilot tests with a special type of RFID infrastructure that is capable of sensing temperature, humidity, and pressure. In these pilot tests, the Navy applied RFID tags to containers carrying high-valued engines in order to know not only their location within plants and warehouses but also to determine when the different characteristics (temperature, humidity, and pressure) changed outside the allowable tolerances. The RFID tags would send information to an asset management system whenever the sensors inside the containers detect a potentially dangerous situation; for example, too high a temperature or too high a humidity level. These pilot tests also proved the ability to transmit location information even when deployed in the field by being offered the capability of the RFID tags communicating with information systems via satellite or cell phone.

1.2.4 Gasoline Payment

A few major oil companies are bringing to market a new, more convenient way to pay for gas. This method employs an RFID tag with a unique identifier that is transferred to the pump via the RFID reader. Once the unique identifier has been read, the back-end information system matches this unique identifier and relates it to the person at the gas pump, providing all of the information to complete the sale. Preference information, such as to what credit card the consumer uses and whether or not the consumer wants a receipt, is stored in the consumer's profile and used at the point of sale (gas pump). Figure 1-1 shows Mobil's Speedpass.

1.2.5 Attraction-Park Children Positioning

A common problem that almost every parent has experienced to some degree is losing a child in a public venue. This is usually a very frightening situation. To alleviate this problem, some attraction parks have established a child-tracking system in which an RFID-enabled bracelet is placed on the child's wrist (see Figure 1-2). RFD readers strategically set throughout the park grounds provide complete coverage so that the child can be found

Figure 1-1 Exxon Mobil's Speedpass RFID solution (Courtesy of CardWeb.com, Inc.).

using various location determining methods (for example, triangulation). This information is secured by the park's information system and is provided only to the person responsible for the child.

1.3 RFID Systems—RFID Infrastructure

The simplest RFID system (or infrastructure, as it is commonly referenced) has three major components, as depicted in Figure 1-3:

- An RFID tag
- An RFID reader
- A predefined protocol definition (format) for the information transferred

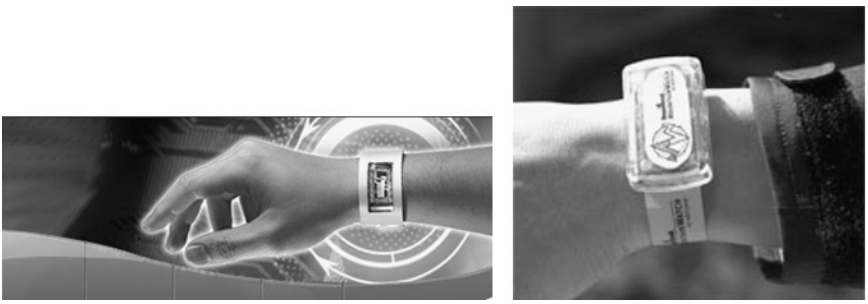

Figure 1-2 RFID-based bracelets (Courtesy of Texas Instruments, Inc.).

Figure 1-3 Simple RFID system.

An optional component, based on the topology of the RFID infrastructure, is what is termed a *signpost* and is discussed in Section 1.3.3. Also, it is important to note that the third component is not a physical component but rather an agreed methodology that allows for the interpretation of the information transferred between the other two components (the RFID tag and reader).

Real-world systems are often more complex than that shown in Figure 1-5 in many respects. One of the promises of RFID is the ability to tie together different organizations, whether they are from within the same enterprise (for example, the manufacturing deparent and the distribution department of a company) or different enterprises (for example, suppliers and customers of an enterprise). The ability to have real-time information across these organizations can bring tremendous value to both parties, but this shared information must be understood by all participants of the information chain. To this effect, RFID systems must be expanded from the simplest form to incorporate other elements that enable the information chain.

These real-world systems employ one or more of the following components:

- RFID middleware and database
- RFID-enabled applications

The addition of these components enables an RFID solution that can interact with enterprise-wide as well as interenterprise information systems. Additionally, as the industry matures, RFID self-governing bodies lead the way for the creation of hardware, software, and data standards that increase the efficiencies of these components. Figure 1-4 shows the interaction of the components.

But before we get to the description of this collaborative environment, it is important to extend our depiction of the basic RFID system.

1.3.1 Tags

Let’s start with the tag. The tag is composed of two essential elements and one optional component:

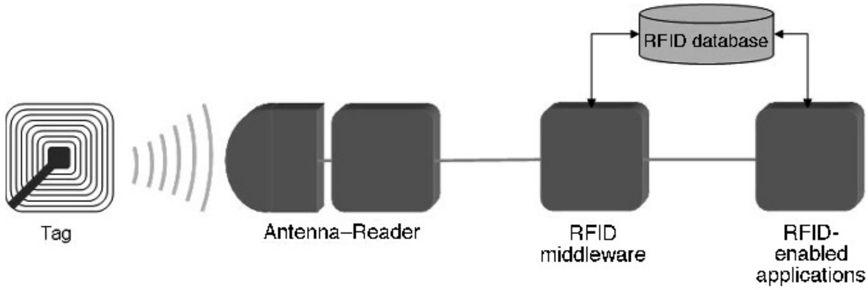

Figure 1-4 Extended RFID infrastructure.

- An integrated circuit,
- An antenna,
- Memory (optional)

The integrated circuit (or IC) contains a microprocessor, memory, and a transponder. The microprocessor processes the information coming from the reader and, at a minimum, accesses the memory to provide the unique identifier for the tag. On this topic, by definition, each tag contains a unique identifier within the predefined protocol definition that makes it different from every other tag in a specific set.

The antenna is used to communicate with the reader and extends the range of this communication. Antenna design varies quite drastically based on the environment and application of the tag. A good antenna design will enable proper communication between the tag and the reader, yielding a very reliable system. Conversely, poor antenna design or incorrect choice of antenna design may negate communication between these components, thus creating high levels of misreads (very poor reliability).

As we will see later in this chapter, some tags provide the ability to remember information sent by the reader. The memory is used for this purpose.

Tags come in three basic flavors:

- Passive tags
- Active tags
- Semi-active tags

They can also be read-only or provide read-write capability.

1.3.1.1 Passive Tags

Passive tags have no built-in power source. Power is provided by the radio frequency wave created by the reader that induces in the antenna a tiny but sufficient electrical current to activate the tag. When the tag comes into the range of the radio frequency wave field created by the reader, it uses that energy to power up its internal components and to communicate with the reader. The advantages of these tags are that they are inexpensive to manufacture, are very small in size, and require no internal power supply. The drawback is that the range of operation (in terms of the distance from the reader) is limited to only a few meters. Figure 1-5 shows various types of passive tags. The antenna configurations vary widely based on the application of the tag. Different configurations work differently based on the constraints of the environment in which the tag will be used. Much experimentation is required to design an effective antenna. In practice, this is usually performed on a trial-and-error basis.

1.3.1.2 Active Tags

Active tags have an internal power source (a battery) that provides the necessary power for the operation of the tag over a period of time. Because active tags beep (in their respective radio frequency) at specified intervals, the battery life is determined by the frequency of the beeps. The higher the beeping frequency (number of beeps in a given period), the shorter the battery life. These tags are constantly beeping (or "chirping," as it is commonly called) and therefore are not required to be within the power field of the reader to be detected. Because they use an internal battery, their signal strength is a lot higher than passive tags and therefore can be read from a further distance. This is one of the advantages of active tags. In open-field environments with minimal interference, active tags can be detected more than 1.5 km away from the reader. The downside of active tags is usually twofold: the cost and the size of the tag. Because they must have a self-contained power source, the cost of the tag is bounded on the lower end by the cost of the battery, which by itself is usually more than the cost of a passive tag. Similarly, the battery takes space, and therefore the tag

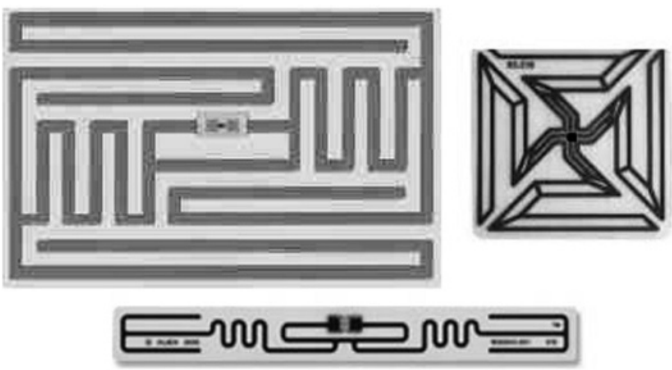

Figure 1-5 Passive RFID tags.

must allocate real estate for the battery. This increases its size dramatically when compared to a passive tag. Figure 1-6 depicts various active tags.

1.3.1.3 Semi-Active Tags

One of the problems with active tags is that their use is bounded by the life of the batteries that power them. Furthermore, frequently beaconing (or, chirping) reduces the life of the battery, so in environments where there is a need for real-time or pseudo-real-time reads, these tags may not last for a sufficient amount of time. A semi-active tag is a combination of a passive and an active tag. The passive component of the tag gets energized as it comes into the electromagnetic field of a reader. As it energizes, it triggers the active component of the tag to send an RFID signal. The benefit is that the battery is only used when triggered by the passive component of the tag, and it then returns to "sleep" mode after a predetermined amount of time, thus halting the battery drain. The signal travels further than if it were originated from a passive tag component, thus, the range of the tag is much higher.

1.3.1.4 Read/Write Tags

Another classification of RFID tags is whether they are *read-only* (RO) tags or they can be *read-write* (RW) tags. RO tags, as their name implies, can only be read by the reader. In other words, the communication between the

Figure 1-6 Active RFID tags (Courtesy of RF-Code, Inc.).

reader and the tag is unidirectional. These tags are encoded with their unique identity at manufacturing time or at initial setup time.

RW tags provide the capability of not only reading information from the tag by the reader but also the ability for the reader to send (write) information to the tag at any time. These types of tags contain a memory space used to store the information sent by the reader. This memory space can vary from just a few bytes to hundreds of kilobytes (KB) and much higher memory capacity is expected in the future.

Whether a tag is RO or RW depends primarily on the type of application in which it will be used. Some applications do not require the tag to hold any information, as it is only used as an identifier. Other applications require information, such as an asset maintenance history, to be maintained by the tag

1.3.2 Readers

Readers are the electronic components that transmit and/or receive the radio frequency waves used to communicate with the tags. Chapter 4 provides more information concerning the types of readers and the physics behind them, but for now it is important to put forth a basic understanding of readers and their components. A reader has two main elements:

- An antenna
- An IC board with at least
- A microprocessor
- Memory
- A radio frequency transponder

1.3.2.1 Antennas

Antennas are the required conduit to receive and transmit radio frequency waves. Much like the radio in a car requires an antenna to receive a signal, a reader must use the antenna to communicate with the tag. Antennas come in a variety of forms and are tuned for the specific environment in which they will be deployed. Figure 1-7 shows some different antenna configurations.

The critical importance of the use of the appropriate antenna cannot be understated in a specific environment for the success or failure of the communication between the tag and the readers. Many otherwise great RFID deployments have failed because of the selection of improper antennas.

1.3.2.2 Reader IC Board

The IC board in the reader processes the necessary information to communicate with the tag. It also uses its transponder to handle the radio frequency communication with the tags. There is a great deal of complexity associated with handling the communication with the tags. Because of this,

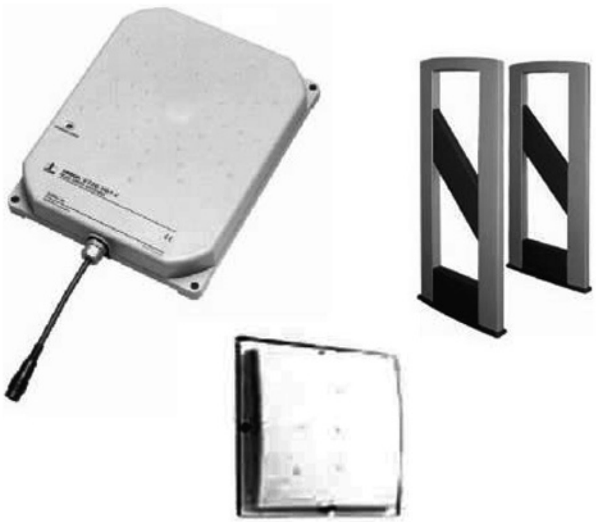

Figure 1-7 Different types of reader antennas (Courtesy of Texas Instruments, Inc.).

readers have microprocessors that allow them to handle a variety of situations when communicating with tags.

One of these situations is what is called a *collision*. A collision occurs when two tags are trying to communicate at exactly the same time with the reader. Since tags are self-contained entities that don't know about other tags (although this is not always true, as we will see when we discuss RFID self-forming networks later in the chapter), they send information to the reader on their own schedule. Because a reader only has one channel of communication, it must handle simultaneous communication (i.e., the collisions) in specific ways. We go into more detail on collisions in Chapter 4. As collision mechanisms develop over time, the microprocessor provides a versatile solution to handle this type of circumstance.

1.3.3 Signpost

A *signpost* is a special transmitter, usually using infrared technology, that can provide granular location information in an RFID infrastructure. Signposts came into being out of necessity. One of the current limitations of general RFID infrastructures is that it is very hard to pinpoint the location of tags due to what is called *RF signal bleeding*. To explain this, consider the following example. Assume that your RFID infrastructure spans multiple floors within a building. Because of the geography of the building, it may be impossible to stop RF signals from being read in the floors above and below a tag. In fact, in three-dimensional space, the closest reader to a tag may be located on the floor above or below it. In an RFID infrastructure, it is almost impossible to discern that a further reader on the same floor as the tag should be used as the correct reader instead of the reader on the floor above or below the tag.

To solve this problem, some vendors have devised a signpost that operates in the infrared spectrum as opposed to operating in the radio frequency spectrum. One very important characteristic of infrared signals is that they require line of sight to be detected—think of a typical TV remote control; if you put your hand in front of its infrared light-emitting bulb, you cannot control the TV. The advantage of the signpost is that it is very inexpensive, so you can put them in many locations in an RFID infrastructure. The tags can read the signal being emitted by the signpost and append it to their ID, thus telling the reader where the tag is. Since infrared requires line of sight, as long as the signpost is enclosed in a "room" (the field covered by the reader), the RFID infrastructure can discern, with granularity, where tags are located.

1.3.4 RFID Information

Traditionally, different vendors of RFID solutions had different methodologies for communicating between readers and tags. Every vendor created what was thought to be the most efficient and complete mechanism for communication. The result was that readers and tags from different vendors could not communicate, thus limiting the possibility of creating complex RFID solutions. In the last few years, several organizations have attempted to create a single standard of communication to facilitate the rapid growth of RFID solutions. Entities such as Massachusetts Institute of Technology's (MIT) Auto-ID lab and the ISO Standards body have provided a platform where teams of RFID providers and users come together to create a standard for interindustry RFID communication. This is thought to be the only means by which RFID can penetrate industrial solutions on a major scale. These standards address many, if not all, aspects of RFID communication, from how the reader and the tags communicate with each other to what information is provided by the RFID infrastructure to the consumer applications.

1.3.4.1 EPC Standards

The Electronic Product Code (EPC) standard was developed by the Auto-ID Center at MIT with the collaboration of academic and industry personnel and currently administered by EPCglobal, Inc. The standard provides a mechanism to uniquely identify every product ever manufactured or to be manufactured. The commonly known Universal Product Code (UPC) provided a mechanism to uniquely identify every *type* of product manufactured but did not allow for the identification of every instance of each of the product types. The EPC does provide for the identification of every instance.

As one can imagine, there are billions, if not trillions of products manufactured in the world (imagine every can of soda, shoe, pencil, and so forth having its own unique EPC numbers). So, the protocol definition to uniquely identify each product must account for the large number of diverse products and instances. To do this, the EPC standard cleverly partitions the manufacturer and product number in a way that is compact and sensible. The key to this protocol definition is the centralized body that dispenses the EPC numbers according to the predefined protocol, much like the GS1 US dispenses the UPC numbers. Figure 1-8 shows an example of an EPC encoding schema. The standards are discussed in much greater detail in Chapter 7.

1.3.4.2 ISO Standards

Another global body in charge of providing different types of industry standards is the well-known International Organization for Standardization (ISO®). This organization, made up of over 140 members from over 90 nations, provides nation-neutral standards that help people from all continents do business with each other on a common platform. ISO has been working on RFID for years; it has released and is currently working on standards to define the communication protocol of RFID components as well as data elements and data interfaces for dealing with RFID information.

Many European businesses opt for ISO as an alternative to what is perceived by some as a U.S.-biased organization, EPCglobal, Inc. However, there is a movement within these organizations to provide a unified standard for true worldwide cooperation.

1.3.5 Self-Forming RFID Networks

A special type of RFID network infrastructure is what's called a *self-forming network*. This infrastructure is made up of tags that can act, beyond their normal capabilities, as relay transceivers that can not only transmit their own information but also relay the information they receive from other tags, thus extending the reading range.

Figure 1-9 shows a pictorial representation of a self-forming network. What is unique about these RFID infrastructures is that the self-forming network can recognize a tag when it comes into the "read" field of the infrastructure, since the tags have the capability to, by using a predefined protocol, recognize other tags and relay their information. The result of this

Figure 1-8 EPC-based information (Courtesy of EPC Global).

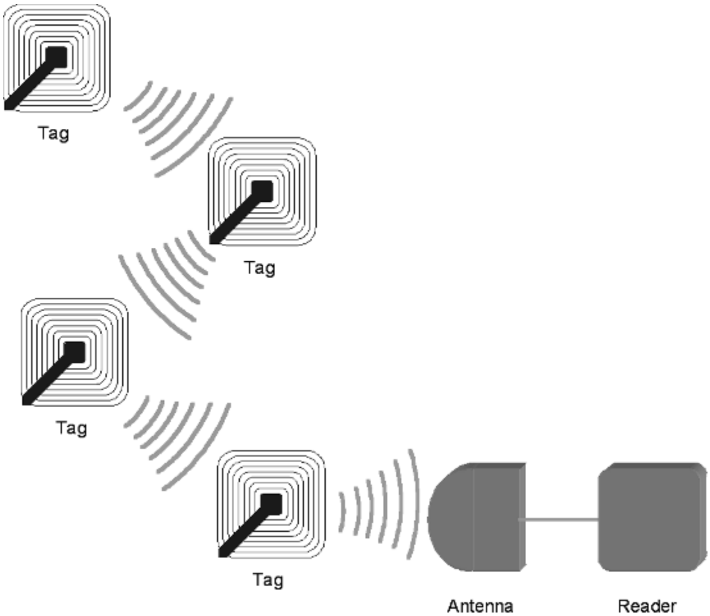

Figure 1-9 Self-forming network.

is that the actual read range of the RFID infrastructure can be extended if there are tags that can relay the information of themselves as well as other tags.

1.3.6 RFID Middleware and Database

Middleware refers to the software component in charge of converting low-level RFID hardware information into usable event information. In other words, the middleware component interfaces with the RFID hardware components (i.e., the readers) and is responsible for translating machine information into information related to tag events. Tag event information refers to the logical events that are mapped to the actual physical events. Although different RFID systems can handle different types of events, there is at least one event that is universal to all RFID systems: "Tag seen by a reader."

This particular event signals the fact that the reader detected a tag. The tag ID is the minimum information reported by the middleware. Usually, this information is also combined with other useful information, such as:

- Tag ID
- Reader ID
- Date/time stamp

The middleware acts as the standard mechanism of communication with readers. This is important because it allows computer information systems and applications to use a higher-level communication methodology with the RFID infrastructure without having to understand the lower-lever issues required to communicate with the RFID hardware.

More sophisticated RFID systems can handle others events. For example:

- Status of tag memory
- Tag sensor information (assumes sensors embedded in tag)
- Tag battery level (applicable to active tags)
- Tag position (assumes GPS or other location feed)
- Tag into zone
- Tag out of zone

Another benefit of middleware components is that they provide for the use of one single mechanism to communicate with different RFID infrastructures. For example, some RFID applications require the capability of deploying both active and passive tags into an environment to provide the proper data capture level. Middleware allows the receiving information systems to just use a single communication protocol to talk to both types of RFID infrastructures. This greatly reduces the IT requirements for this type of RFID solution.

Because RFID systems tend to generate huge amounts of tag event information, it is important to provide a mechanism that allows asynchronous communication with the RFID system. The middleware component makes use of an RFID database to keep track of the different types of tag events generated by the infrastructure and then to analyze correlated events to provide higher-level logical events. An example of this may be the "tag into zone" event. This is in reality a logical event that is composed of a sequence of physical events.

To illustrate this example, let's assume that we want to know when an active tag, beeping at an interval of once every two seconds, came into a specific zone. Furthermore, let's assume that this zone is defined by a room that is 100 percent covered by a reader. Figure 1-10 shows a picture of this scenario. When the tag is out of the room, the reader cannot detect anything and thus reports nothing. As soon as the tag enter the room, the reader informs the middleware that Tag X has been seen. In our example, the reader will detect the beep from the tag every two seconds and will report that information to the middleware (every two seconds). If the tag is left in the room for a period of 10 hours, the reader would have sent 18,000 messages (30 messages/minute $\times$ 60 minutes/hour $\times$ 10 hours) to the middleware telling it that it saw the tag all of those times. An information system is probably not ready to handle that kind of volume of data, nor is it interested in handling it. The middleware can greatly improve this process by being a bit smart and providing just the logical information of interest to the information system—that is, an asset went into the room. As long as

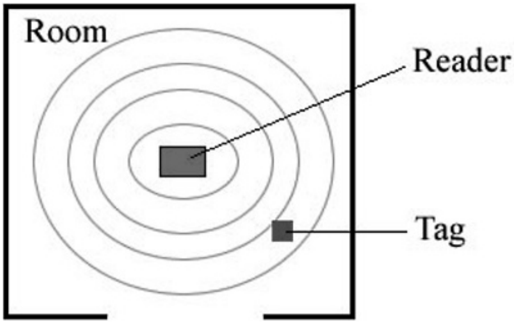

Figure 1-10 "Tag into zone" event.

the tag is still in the room, it is not really necessary to keep telling the information system that the tag it is still in the room, unless, of course, the information system is interested in verifying that the tag is indeed in the room.

The "tag into zone" event is composed of the following physical events:

- A tag is detected by a reader covering a zone.
- The tag continues to be detected by the same reader for some period of time.

In this case, the middleware is probably using the RFID database to check the tag id and the date/time stamp received from the reader and comparing it against what is in the database. For example, assume that the same tag had been seen by the same reader within the last few instances, but it had not been seen previously. It can be assumed that the tag came into the zone, thus reporting a "tag into zone" event to the information system. From then on, the "seen" event reported by the same tag, can be properly ignored and not communicated to the information system. So, in this example, the information system would only receive one message from the middleware ("tag into zone"), as opposed to 18,000 messages stating that reader *Y* saw tag *X*.

1.3.7 RFID-Enabled Applications

In actuality, RFID applications are not truly part of an RFID infrastructure but rather the recipient of the information provided by the RFID infrastructure. However it is important to mention them in this section, since these applications are the consumers of the information and act upon this information. These applications could be any system that uses the RFID information and processes it in some way. Following are examples of these:

- Warehouse management systems (WMS)
- Transportation management systems (TMS)

- Production scheduling systems
- Order management systems (OMS)
- Order entry systems (OES)
- Inventory management systems
- Asset management systems

These applications must be written (or re-written, in many cases) to accept real time data pertinent to the RFID infrastructure.

1.4 RFID in the Enterprise

With the basics of RFID explained, practitioners of industry will demand to know how and where does RFID fit in the enterprise. As illustrated in Section 1.2, there are already many applications where RFID creates a lot of value, whether by providing a cost savings opportunity, improving service levels, or actually increasing revenue.

Before implementing an RFID solution, there are many questions that must be answered. Business managers will want to consider, among other items:

- Compatibility of the solution with the environment
- The potential ROI
- The risk factors associated with using new or newer technology
- The IT capability to handle RFID-generated massive volumes of data
- The state of readiness of systems interacting with the RFID solution (or, infrastructure)
- Applicability of the RFID solution as opposed to other less technically challenging solutions

In many instances an RFID solution will be much more appropriate if combined with other technologies, such as bar codes, in order to provide a fail-safe, redundant solution. In other instances, RFID solutions may not be the most appropriate because of environmental, economic, or safety reasons. The point is that in every instance a detailed feasibility analysis must be conducted in order to determine the viability of an RFID solution. This section contains a list of questions and issues that should help the practitioner determine if RFID is the most appropriate solution for the problem at hand.

1.4.1 Why, When, and Where RFID?

The three basic questions to determine whether RFID should be considered as a potential solution are *why, when,* and *where* should an enterprise deploy

RFID. These are considered "strategic" questions, and their answers should be clearly understood before asking the operational questions of *how* should the enterprise deploy an RFID solution? They are considered strategic because their responses will dictate whether or not an enterprise will embark into a, more than likely, long-term project that will require considerable (and specialized) resources, money, and time. If these answers are not clearly understood before commencing the project, project members will face uncertainty throughout the project and the possibility of project failure increases rather dramatically. The *how* question should be a surrogate to the strategic questions. It is not to say that it is any less important, but it is not sufficient. To illustrate this point, think of an asset-tracking project where the price of the tags is too high compared to the products being tracked. In this case, an implementation engineer may know exactly how to implement the RFID-based asset tracking solution, but it would not make sense from an ROI point of view.

Although *why, where,* and *when* questions are a good staring point, they should be broken down into more detailed questions for proper analysis. The following is a list of questions that expands on these strategic questions and is useful in making a high-level determination on the viability of an RFID solution:

- What is the value provided by the RFID solution?
  - Cost reduction
  - Revenue generation
  - Productivity or process improvement
  - Marketing differentiator
  - Service improvement
  - Vendor/supplier mandate
  - Quality assurance
- Do individual objects need to be uniquely identified?
  - If there is no need to track objects, it may be doubtful that an RFID solution would be useful.
- Is the environment where objects need to be tracked a closed-loop environment or an open environment?
  - This may dictate the type of RFID technology to be used in terms of the infrastructure required.
- Is there a need for real time or near-real-time data capture?
  - If not, there may be other less sophisticated solutions that may provide the necessary results at a lower cost.
- What are the physical characteristics of the objects to be tracked?
  - Characteristics such as size, liquid content, metal content radio frequency interference, and others will dictate the type of RFID solution to be used.

- What is the universe of objects to be tracked?
  - How many?
  - What types?
  - Over what area?
- Are the interfacing information systems able to handle massive volumes of RFID-based information?
  - Typically, RFID systems generate huge amounts of information for processing by other systems. It is important to understand how these other systems will face such amounts of data.

As we will see in Chapter 6, one of the most important steps in the determination of the applicability of RFID solutions is the computation of the ROI. This is many times an elusive subject, since the components of the computation are sometimes soft (qualitative) and sometimes hard (quantitative). This is especially true when the benefits of an RFID solution are more qualitative than quantitative, as, for example, in the case of improved customer service or marketing differentiation.

1.4.2 A Road Map to Implementation

The implementation of an RFID solution deals primarily with the *how* question. Once the strategic questions (*why, where,* and *when*) have been clearly addressed, the implementation teams must put in place a project plan that will cover every aspect of the installation and operation of the RFD solution. As any other project, implementing an RFID solution requires detailed analysis of the problem at hand and the proposed solution. The following is a high-level implementation guideline:

- *Identification of problem at hand*
  - Documentation of problem characteristics and issues
  - Identification of parties involved in the problem (vendors, customer, partners, etc.)
  - Identification of the environment involved in the problem (physical characteristics of environment)
    - High metal content; this will create interference and limit the range of RFID.
    - High water or liquid content; water, or liquids for that matter, block and deflect radio frequencies, this increases misreads of RFID signals.
    - High radio frequency areas; areas in which there is a high concentration of electro-magnetic waves (microwaves, radio-broadcasting, TV signal emitters, etc.) will create interference with the RFID signal thus limiting the reliability of the system.
    - Areas where there is radio wave sensitive equipment, such as medical telemetry equipment, electronically controlled explosives, sen-

        sitive navigation systems, and so forth, can be affected by RFID signals.
        - All these will have a profound effect on the type of RFID solution applicable.
    - Identification of IT systems involved in the problem (input, output, consumer, and transactional IT systems and interfaces)
    - Identification of high-risk issues
        - Time-driven constraints related to infrastructure deployment-building requirements, if any
- *Business case analysis*
    - Identification of cost components
    - Identification of benefits
    - ROI analysis
- *Definition of solution implementation team*
    - Business process owners
    - User representative members
    - Information technology members
    - Facilities manager members
    - Vendor/provider members
- *Design of solution*
    - Documentation of solutions components
        - Infrastructure specification (wired, wireless, mixed)
        - Readers (with associated hardware)
        - Tags (with associated hardware)
        - Antennas (with associated hardware)
        - Custom casing for components
        - Cabling
        - Wireless equipment
        - Power requirements and power supply points
        - Computer hardware such as servers, backups, uninterruptible power supplies
        - Local or wide area network requirements (port drops, etc.)
        - Communication requirements (satellite, cell-phone, etc.)
    - Documentation of business process requirements
        - Process changes
        - Process additions
        - Process eliminations
    - RFID event definitions
        - One of the most important aspects of an RFID solution is the issue of what events need to be tracked.
    - Definition and documentation of IT requirements and interfaces
        - Data generation systems—systems that provide information to the RFID infrastructure
        - RFID database contents—systems that maintain transient RFID event information

    - RFID history data warehouse—systems that maintain historical RFID event information
    - Processing systems—systems that convert or enhance RFID event information
    - RFID data consuming systems—systems that utilize RFID event information to provide decision support capability
  - Catalog of vendors available for RFID solution
    - This may be the hardest task given the fact that the industry is in its infancy. Market hype tends to be emphasized over practical experience, although many of the RFID solutions deployed are the first of their kind.
- *Pilot test phase—Selection of problem subset to test solution*
  - Definition of pilot test's objectives. The pilot test may have multiple objectives, for example:
    - Testing of new technology or multiple competing technologies
    - Testing of coverage area
    - Testing of environmental fit; how well does the RFID solution work in a specific environment?
    - Testing of system reliability
    - Testing of system interfacing
    - Testing of data processing scalability (given the huge amounts of data produced by the RFID infrastructure)
  - Definition of pilot's scope such as
    - Objects to track
    - Coverage area
    - Events
    - Interfacing information systems
    - Personnel
    - Business processes
  - Setup of baseline against which results will be measured
    - This process is extremely important to understanding the success or failure of the pilot test. This also dictates the clear definition (as stated previously) of the pilot test's objective.
- *Adjustment of solution based on pilot test's feedback*
  - Stress test solution for abnormal situations
    - Power failure
    - Network failure
    - Server failure
    - Extraneous tags
    - Reader failure
    - Tag failure
  - Adjustment of infrastructure (antenna positioning, reader strength and setting, tag enclosures, etc.)
- *Roll out of solution in phased approach*
  - Schedule of rollout:

        - Personnel
        - Coverage area
        - Products tagged
        - Events tracked
    - Business process change requirements
- *Normal operation*
    - Continuous improvement methodology