RFID offers tantalizing benefits for supply chain management, inventory control, and many other applications. Find out whether your company could benefit.

Ron Weinstein

RFID: A Technical Overview and Its Application to the Enterprise

Radio frequency identification (RFID) has been around for decades. Only recently, however, has the convergence of lower cost and increased capabilities made businesses take a hard look at what RFID can do for them. A major push came when retailing giant Wal-Mart dramatically announced that it would require its top 100 suppliers to supply RFID-enabled shipments by January 2005. Though the bottom line story of that deployment has yet to surface, it does seem to support the inevitable movement of inventory tracking and supply chain management toward RFID.

This article offers an RFID tutorial that answers the following questions:

- What is RFID, and how does it work?
- What are some applications of RFID?
- What are some challenges and problems in RFID technology and implementation?
- How have some organizations implemented RFID?

Answering these questions will provide an organizational framework for RFID implementation from both the technical and business perspectives.

Inside

TECHNICAL OVERVIEW

The basic premise behind RFID systems is that you mark items with tags. These tags contain transponders that emit messages readable by specialized RFID readers. Most RFID tags store some sort of identification number; for example a customer number or product SKU (stock-keeping unit) code. A reader retrieves information about the ID number from a database, and acts upon it accordingly. RFID tags can also contain writable memory, which can store information for transfer to various RFID readers in different locations. This information can track the movement of the tagged item, making that information available to each reader ("A Guide to Understanding RFID," *RFID J.,* retrieved 27 Feb. 2005; http://www.rfidjournal.com/article/gettingstarted/).

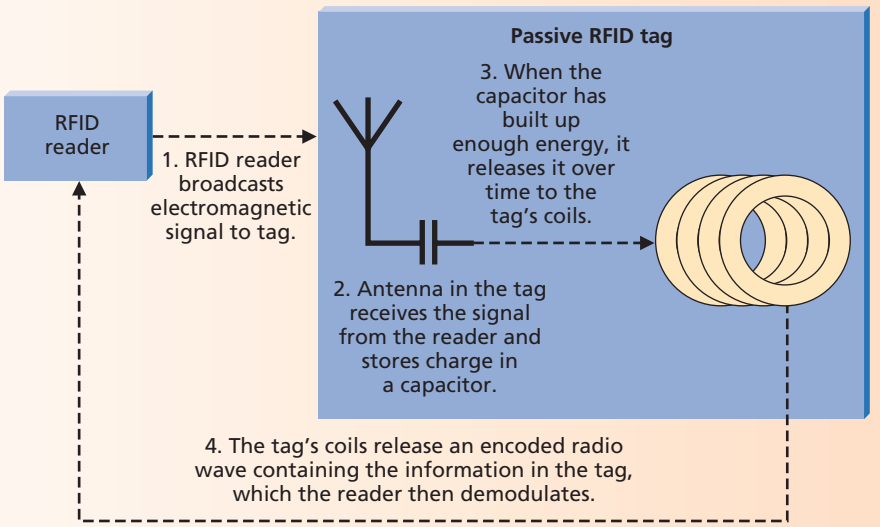
RFID tags fall into two general categories, active and passive, depending on their source of electrical power. Active RFID tags contain their own power source, usually an on-board battery. Passive tags obtain power from the signal of an external reader. RFID readers also come in active and passive varieties, depending on the type of tag they read.

Active tags

Because they have their own power source, active tags transmit a stronger signal, and readers can access them from further away. The on-board

1520-9202/05/$20.00 © 2005 IEEE Published by the IEEE Computer Society

Figure 1. Simplified view of data transfer in low-frequency passive RFID tags (the tag is enlarged for clarity).



power source makes them larger and more expensive, so active RFID systems typically work best on large items tracked over long distances. Low-power active tags are usually slightly larger than a deck of playing cards. Active tags can remain dormant until they come in range of a receiver or can constantly broadcast a signal.

Because of their on-board power source, active tags operate at higher frequencies—commonly 455 MHz, 2.45 GHz, or 5.8 GHz—depending on the application's read range and memory requirements. Readers can communicate with active RFID tags across 20 to 100 meters.

Passive tags

Passive tags, on the other hand, are very inexpensive; they can cost as little as 20 cents apiece, and new technologies are constantly making them cheaper to integrate into common materials and products. Because passive tags are inexpensive, they will likely be the basis of most of the growth in RFID implementations, so I will examine the technology behind passive tags in detail.

In addition to their low cost, passive tags can also be quite small. Current antenna technology limits the smallest useful passive tag to about the size of a quarter. The larger the tag, the larger the read range.

Currently, passive RFID tags contain about 2 Kbits of memory. This is too small to hold much more complex information than identification and history information. The technology behind RFID is constantly improving, so the amount of information and capabilities of RFID tags will increase over time, allowing RFID tags to eventually contain and transmit much more information.

A passive-tag reader can constantly broadcast its signal or broadcast it on demand. When a tag comes within the reader's range, it receives an electromagnetic signal from the reader through the tag's antenna. The tag then stores the energy from the signal in an on-board capacitor, a process called *inductive coupling*. When the capacitor has built up enough charge, it can power the RFID tag's circuitry, which transmits a modulated signal to the reader. That return signal contains the information stored in the tag.

The communication between the reader and passive tag uses one of two methods to modulate the ID signal. Low-frequency (less than 100 MHz) tags pass information by releasing energy from the capacitor to the tag coils in varying strengths over time, which affects the radio frequency emitted by the tag. The reader detects these varying waves and can use these variances to demodulate the code. Figure 1 shows this *load modulation*.

In higher-frequency (greater than 100 MHz) tags, the tag transmits the signal using *backscatter*, in which the tag's circuit changes the resistance of the tag's antenna. This change in resistance causes a transmission of RF waves, which the reader can pick up and demodulate. Passive tags typically operate at frequencies of 128 KHz, 13.6 MHz, 915 MHz, or 2.45 GHz, and have read ranges of a few inches to 30 feet. Frequency choice depends on the system's environment, what material the signal must travel through, and the system's required read range.

RFID tags can be encased in many materials. Plastics are a very common material for RFID, forming identification cards for building access, credit cards, or bus fares. Tags can also go on the back of labels printed on standard ink jet printers, for placement on inventory.

STANDARDS

Several RFID standards exist, and their applications are under debate within the RFID development community. These standards cover

- identification, the coding of unique item identifiers, or other data on the RF tag;
- data and system protocols, effectively the middleware of an RFID system;

- the air interface, that is, the wireless communication between the reader and the tag;
- application support, which provides advice about how to implement the technology;
- testing, compliance, and health and safety, that is, the rules that govern RFID operations; and
- terminology.

The International Standards Organization (ISO) has three standards for RFID: ISO 14443 (for contactless systems), ISO 15693 (for vicinity systems, such as ID badges), and ISO 18000 (to specify the air interface for a variety of RFID applications). A not-for-profit organization, EPCglobal, has developed a widely accepted standard for product identification. The Electronic Product Code (EPC) standard covers the air interfaces, the format for the product identification data stored in an RFID tag, and the middleware and databases storing information about the tags.

The US Department of Defense now requires suppliers to use RFID "on lowest possible piece part/case/pallet packaging once the supplier's contract contains language regarding the requirement" (http://www.dodrfid.org). The DoD specifies EPCglobal or compatible tags. In 2004, the DoD ran a field test RFID deployment, as the "US Navy RFID Pilot" sidebar describes.

EPCglobal has developed a system called the Object Naming Service (ONS) that is similar to the Domain Name Service (DNS) used on the Internet. ONS acts as a directory service for organizations wishing to look up product numbers (also known as EPC numbers) on the Internet. EPCglobal awarded VeriSign a contract to manage ONS in January 2004. ("VeriSign to Run EPC Directory," *RFID J.*, 13 Jan. 2004; http://www.rfidjournal.com/article/view/735/). In reports dated January, 2004, Wal-Mart, though a member company of EPCglobal, reported that it has no plans to use the ONS service, opting to use its own proprietary database and formats.

In terms of the all important air interface, ISO 18000 and the EPC standard were incompatible. However, in January 2005, EPCglobal submitted its UHF Class 1 Generation 2 Specification for possible inclusion in the ISO standards. The National RFID Centre, an initiative of the UK Department of Trade and Industry, hailed the move as a much needed convergence of international RFID standards ("Convergence of RFID Standardisation Efforts," 13 Jan. 2005, http://www.rfiduk. org/news/view. php?id=3).

US Navy RFID Pilot

In May 2004, the US Navy finished its pilot of a passive-RFID system to support the loading of supplies into cargo containers. The pilot project took place at the Fleet and Industrial Supply Center (FISC) in Norfolk, Virginia; the original goal was to reduce the number of errors in records of supplies loaded into the containers. These errors arose from manual and/or nominally automated data inputs in the standing process. For the pilot, FISC used passive tags read as a forklift carrying the supplies (shipments) passed through specially equipped portals. In all, FISC spent $306,000, or 93 cents per shipment during this pilot.

In its final configuration, the RFID-enhanced process also increased the speed and efficiency of the cargo checking process. Although the pilot's goal did not include a return-on-investment justification, the final report indicates that "as many as twelve additional personnel could conceptually be assigned as additional drivers, or to work in other functions within the operation" because monitoring the RFID pilot system did not require as many people as the legacy system. In the process, FISC learned several valuable lessons that would apply to similar RFID deployments. The report *Final Report of the Passive Radio-Frequency Identification (RFID) Project at the Fleet and Industrial Supply Center, Norfolk, Virginia, Ocean Terminal* describes those lessons and the pilot project in detail (http://www.acq.osd.mil/log/logistics_materiel_readiness/organizations/sci/rfid/assetts/Meetings/FISC%20Norfolk%20OT%20Report%20v8.pdf).

Figure 2. Common devices that employ RFID.

Some car keys (upper left) contain a passive tag. An EzPass (upper right) helps collect highway tolls, a SmarTrip card (bottom) collects fares in a public transit system.

BUSINESS APPLICATIONS

RFID applications are numerous and far reaching. The most interesting and widely used applications include those for supply chain management, security, and the tracking of important objects and personnel.

Supply chain management

In supply chain management, RFID tags are used to track products throughout the supply chain—from supplier delivery, to warehouse stock and point of sale. New applications target tracking from checkout through customer billing. A central database records product movement, which manufacturers or retailers can later query for location, delivery confirmation, or theft prevention.

For this application, RFID basically serves as a replacement for the bar code scanners used to track products and shipments in similar ways. Gao and colleagues outlines four ways in which RFID is superior to bar codes for tracking inventory flow over the supply chain ("An Approach to Security and Privacy of RFID System for Supply Chain," X. Gao and colleagues, *Proc. IEEE Int'l Conf. E-Commerce Technology for Dynamic E-Business*, 2004):

- RFID does not require line-of-sight access to read the tag.
- The read range of RFID is larger than that of a bar code reader.
- Readers can simultaneously communicate with multiple RFID tags. Because of this capability, an RFID reader can capture the contents of an entire shipment as it is loaded into a warehouse or shipping container. A reader collects detail information in one pass, without having to scan each product.
- Tags can store more data than bar codes.

The last capability has several interesting applications in supply chain management. For example, read-write tags can store information about their environment. They can physically store their position and time throughout their movement in the supply chain.

An example of a proposed use of RFID is to ensure safety in the supply chain. A US Food and Drug Administration (FDA) proposal supports using RFID to ensure the authenticity of prescription drugs. In this system, each drug shipment would carry a read-only RFID tag containing a unique serial number. Suppliers would track these serial numbers in shipment and have the drug purchaser verify the numbers on receipt, ensuring that the drugs came from where they were expected and arrived at their intended point of sale. The FDA realized that this is rather difficult to implement in such a large and supply chain as that for prescription drugs and proposed a three-year schedule for investigating the technology, ending in 2007, before it sets any policies (*Combating Counterfeit Drugs*, US Food and Drug Administration, Feb. 2004; http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html#radiofrequency).

A correlation to the supply chain management application is to enable automated just-in-time product shipments. If all products in a retail store and associated warehouses have RFID tags, a store should have an accurate database of its inventory. Systems in retail outlets could automatically alert a warehouse management system that inventories are low. The warehouse management system could locate the products in the warehouse based on their initial scan, and automatically move them to a loading dock for shipping to the retail outlet. Wal-Mart is implementing such a system.

Security

Security and personal identification applications are a major and broad application of RFID. A common use of RFID is in identification cards to control building access. Many organizations use RFID tags embedded in ID cards, which are readable at a building entrance.

On a similar note, some credit cards (American Express' ExpressPay, http://www.americanexpress.com/expresspay) and other payment devices, such as ExxonMobil's Speedpass (http://www.speedpass.com), use RFID tags. Other cards use tags for automatic fare payment in mass-transit systems, such as the SmarTrip card for the Washington DC area subway and bus system (http://www.wmata.com/riding/smartrip.cfm). Figure 2 shows samples of such cards. Essentially, these are a replacement for identification cards with magnetic stripes, providing a more reliable way to store identification information—magnetic stripes tend to wear out and lose information over time. RFID tags also have a higher memory capacity than magnetic stripes.

Keys for new cars also incorporate passive RFID tags that work with a reader near the car's ignition switch. The reader will only accept codes stored in certain keys. If the code in a key does not match the reader in the car, the car will not start, making it more difficult to steal vehicles by copying keys.

Movement tracking

Because moving objects can easily carry RFID tags, a common use is to track the movement of people and the information associated with them. Some hospitals now use tags on newborns, to ensure identification and to alert hospital staff should someone attempt to take the baby outside of the hospital without authorization. Some schools are requiring children to wear tag-embedded bracelets or wrist bands while on school grounds, to monitor attendance and to locate lost children ("Tagging Toddlers and Toothpaste," *Information Management J.*, Sept.-Oct. 2004). The FDA recently approved a RFID tag that could stay with surgical patients in hospitals and store information on the surgical procedure the person requires, eliminating surprisingly common surgical mistakes ("FDA Approves Surgical ID Tag," S. Lawrence, *eWeek*, Nov. 2004; http://www.eweek.com/article2/0,1759,1731402,00.asp). This application of RFID has obvious privacy issues, as I will discuss later.

In the same way, tags can track the movement of highly mobile objects in areas other than an organization's supply chain. For example, one large Las Vegas casino plans to place passive tags in each gaming chip, and have readers at cashier stations and gaming tables. In this way, the casino can detect counterfeit chips, and track the movement of chips and player activity ("Vegas Casino Bets on RFID," A. Gilbert, 9 Feb. 2005, http://news.com.com/Vegas+casino+bets+on+RFID/2100-7355_3-5568288.html?tag=nefd.top).

Hospitals are also using RFID to track equipment throughout a facility as it moves from room to room. This helps manage inventory and ensure the proper maintenance of equipment. Libraries also tag books, making it possible to easily locate a book in the stacks, prevent theft, and automate the checkout process.

CHALLENGES AND ISSUES IN RFID

Although promising, RFID is not without its challenges, which arise from both a technological and usage point of view.

Privacy concerns

A common concern with RFID is privacy. It is disconcerting for many people to have their movements or buying habits automatically tracked electronically. Many privacy groups are concerned about the ability to identify people as they walk through a store or shopping center via the tags embedded in their clothing and linked to them at the time of purchase.

To counter such concerns, RFID proponents propose that retail tags have "kill switches" that disable the tag at the point of sale. Even though a small tag might remain embedded inside a product, once the kill switch is activated, the tag would no longer transmit information ("Some Methods for Privacy in RFID Communication," R. Fishkin and B. Jiang, *Intel Research*; http:// www.intel-research.net/Publications/Seattle/062420041517_243.pdf).

Many of the privacy concerns regarding RFID are addressable because of the nature of RFID tags themselves. The read range of RFID tags is much too small to allow readers out of personal range to read tags carried on a person or in a vehicle. Also, building materials tend to absorb the relatively weak RF waves transmitted by passive tags, making it extremely difficult to pick up RFID signals through the walls of a home ("RFID Privacy Workshop: Concerns, Consensus, and Questions," S. Weiss, *IEEE Security & Privacy*, Mar.-Apr. 2004).

However, anytime someone automatically stores and tracks personal identification in electronic databases, privacy concerns are very real. RFID tags used in transportation systems—whether for fare collection on mass transit systems or automatic toll payment on bridges and

Resources for RFID Products

- **Association for Automatic Identification and Mobility (AIM, http://www.aimglobal.org/technologies/rfid): A trade association, AIM focuses on automatic identification; its site includes a buyer's guide to RFID hardware and a solution provider evaluation guide.**
- **RFID Gazette (http://www.rfidgazette.org): A blog, the Gazette reviews RFID products and implementations.**
- **Sybase RFID Platform (http://www.sybase.com/rfid): An example RFID middleware implementation.**
- **The RFID Handbook (http://rfid-handbook.com): The home page for the book contains links to many companies providing RFID products and solutions.**

Tutorials

- **"A Guide to Understanding RFID," *RFID J.*; http://www.rfidjournal.com/article/gettingstarted/.**
- **"RFID 101," W. Singer, *Logistics Today*, Nov. 2004.**
- **"The Magic of RFID," R. Want, *ACM Queue*, Oct. 2004.**

highways—allows for the easy and unprecedented tracking of movement. If you can pay for products in an RFID tag and companies later bill you automatically, it takes all possible anonymity out of the retail process. Companies and government agencies must address these concerns before the public will truly feel comfortable using RFID systems. People will want to see policies about the use of an RFID system and the information it collects.

Security

Security is another key issue in RFID. An organization that implements RFID in its supply chain does not want competitors to track its shipments and inventory. People who use devices that carry personal financial information, such as credit card or other ID numbers, do not want others to access their accounts. These are significant security vulnerabilities in RFID.

Some researchers have proposed schemes that would require tags to authenticate readers, transmitting information only to authorized readers. The tags would have to store ID numbers for authorized readers, and a reader would have to broadcast its ID to the tag. To protect the reader's ID—and prevent others from eavesdropping and stealing the information—the reader uses either a fixed or randomly generated number to hash (encrypt) its ID (Gao and colleagues).

If the tag cannot authenticate the reader's identity, the tag will refuse to transmit the information it stores. Like most security tactics, this scheme is vulnerable to attacks, such as man in the middle, or reverse engineering.

Integration with legacy systems

Another challenge to RFID is its integration into existing systems. Several vendors are developing RFID middleware that will link new RFID systems into existing back-end infrastructures. Middleware, for example, can help with the current lack of standards in RFID. If an organization picks a standard that changes or loses its market prevalence, middleware can transform the data from readers into the format supported by back-end systems. Many RFID middleware systems provide hooks into operational monitors, so organizations can monitor their tagged items in real time ("RFID Anywhere: Leapfrogging the Challenges of RFID Deployment," Sybase Inc.; http://sybase.com/detail?id=1034549). Middleware can provide the primary link between RFID readers and databases.

WAL-MART: TAKING THE LEAD IN RFID FOR RETAIL

Of the many organizations having implemented RFID, the one that received the most media attention is Wal-Mart. The world's largest retailer, Wal-Mart has one of the most

efficient supply chains in the world. With a large array of suppliers from many different industries, Wal-Mart's RFID effort has the potential to cause a web of RFID implementations. One estimate puts Wal-Mart's savings at $8.35 billion per year if it fully implemented RFID throughout its operations. That figure is more than the total revenue of half the companies on the Fortune 500 ("Case Study: Wal-Mart's Race for RFID," M. Roberti, eWeek, Sept. 2003; http://www.eweek.com/article2/0,1759,1492297,00.asp).

Though this savings is substantial, Wal-Mart has taken its RFID implementation fairly slowly. In 11 June 2003, Wal-Mart announced that it would require its top 100 suppliers to tag all cases and pallets by January 2005. This directive sent a wave of panic among suppliers, who scurried to learn about RFID and how best to implement the technology.

Wal-Mart and its suppliers quickly found several challenges in its RFID implementation, namely that the UHF frequency they were using as a standard would not pass through many common products shipped to retail stores, such as water-based products and products shipped in metal packaging. This forced Wal-Mart to back off slightly and relax its deadline for full RFID implementation. By January 2005, the top 100 suppliers had only tagged about 60 percent of their products. Wal-Mart, though, was the first major retailer to implement RFID throughout the supply chain, and force its suppliers to implement RFID as well, so it's natural to have some problems. Wal-Mart's early adopter implementation forced the industry to learn about the challenges in RFID ("Wal-Mart Gives Suppliers RFID Holiday Gift, E. Schuman, *eWeek*, Dec. 2004; http://www.eweek.com/article2/0,1759,1744834,00.asp).

Wal-Mart provides information about its RFID efforts at http://www.walmartstores.com/wmstore/wmstores/Mainsupplier.jsp?pagetype=supplier&categoryOID=10605&catID=-8250&template=DisplayAllContents.jsp.

RFID, a technology existing for years, has potential uses in a variety of applications. Though not without issues and challenges, RFID is a promising technology which analysts expect to become ubiquitous in the coming years, helping organizations solve problems in supply chain management, security, personal identification, and asset tracking. ■

Ron Weinstein *is a graduate student at Johns Hopkins University. He also works for Sybase as a consultant. Contact him at ron@ronsweinstein.com*

For further information on this or any other computing topic, visit our Digital Library at http://www.computer.org/publications/dlib.