RFID: A Brief Technology Analysis

Roger Smith
CTOnet.org

Introduction

Radio frequency identification (RFID) systems have been deployed in limited numbers for years. Two of the most predominant have been in the form of toll road collection transponders and security badges. Toll road authorities around the country have equipped drivers with a transponder that is connected to their credit card. This allows them to pay their tolls at 40 miles-per-hour rather than stopping to throw quarters into a basket and slow the flow of traffic. Security badges have been equipped with RFID chips to allow centralized control of access to facilities and specific rooms within buildings. These can also be used to track the locations of people in a facility by identifying the door they last passed through.

More recently, Wal-Mart and the Department of Defense have kicked the RFID industry into high gear by announcing that all of their suppliers must tag shipping containers with the devices (Angeles, 2005). Wal-Mart has imposed this on their top 100 suppliers beginning in January 2005. At this point, the requirement applies to shipping containers and does not extend to individual product packages. The influence of these two big customers is causing all companies to evaluate whether they should begin adopting RFID tagging systems. Both organizations maintain that RFID tags will improve their performance in moving products, reduce the costs of managing them, and reduce product losses.

Applications

Though tagging shipping containers is certainly a very large business space for RFID, there are a number of other places to apply the technology as well. Some of these are:

- RFID Passports. U.S. Customs is considering attaching an RFID tag to all passports that enter the U.S. and then matching those with the RFID tagged passports that leave the country. This would provide a more consistent and reliable method of determining when people leave the country (Chabrow, 2005).
- Golf Balls. Radar Golf Inc. is embedding RFID tags in the center of golf balls to aid golfers in finding their wayward balls (LaPedus, 2005).
- All Sports Balls. The tags have also found their way into National Hockey League pucks and may find their way into footballs, baseballs, tennis balls, soccer balls and every other form of ball. These can be used to record movement, assist referees, and enhance television coverage.
- Office Folders. A Georgia juvenile court is considering tagging every file in their system. The goal is to eliminate many hours of searching for lost files every week and the resultant impact on court appearances (Sullivan, 2005).
- Micro-sensors are an intriguing new technology. These sensors vary from the size of a deck of cards to the size of a die or small pebble. But one challenge is in keeping

track of where these small devices are located. RFID tags are being integrated into the packages to keep track of them (Ricadela, 2005).

- Aircraft Maintenance. The latest Airbus A380 aircraft have a tag on every component on the aircraft. These were initially intended to aid in maintenance records, but airlines are seeking ways to expand this application now that the tags are on-board (Malykina, 2005).
- Livestock are tracked through the shipping and slaughtering process. This is very useful when one cow is discovered with a disease. It can lead to the identification of the other cattle or beef products that were raised and shipped with the infected animal.
- Humans. Tagging patients in hospitals or bodies in a morgue can be enhanced with the technology (Kanellos, 2004).
- Library books are already being tracked and checked out using RFIDs (Molnar, 2004).
- Kids Games. A number of kid's games have been developed with the technology, the first being Zowie, followed by MusicBlocks, PingPongPlus, and Tagaboo (Konkel, 2004).
- Port Management. The port of Singapore has installed a grid of RFID sensors in the asphalt of the entire port. This allows them to track the location of containers, but also to understand the traffic patterns in the port and improve its performance (Angeles, 2005).

These are just a few of the applications that have been achieved or considered so far. There will be thousands of others as the technology becomes better understood, lower priced, and available as part of other business systems.

How do RFID systems work?

A typical RFID tag contains three components – the chip, the antenna, and the enclosure. The chip stores the unique data associated with the tag. The antenna receives query signals for a tag reader and transmits the internal data from the chip. The enclosure is the packaging around the electronic components. Currently, most chips are manufactured, assembled, and applied to the product packaging. However, in the search of lower costs and ease of deployment, many organizations are creating methods to print a tag right onto a package or embed it in the packaging materials. The process is similar to traditional ink jet printing, but uses metallic-based liquids that can form electronic components (REFERENCE).

Tags are generally categorized as either passive or active. A passive chip is created with a unique identification number in it. The contents of the chip can never be changed and the ID number is released to a reader when queried. The ID number is then transferred into a computer system containing a database in which the ID is associated with product characteristics. An active chip, on the other hand, may contain a great deal more information and this information can be written, erased, and rewritten from an external read/write device. These chips can contain a history of transactions with read/writers that tracks their progress through a supply chain, medical treatment, or any other process.

These chips are considerably more expensive and require security measures to insure that hackers are not changing the contents of the chip.

Technical Challenges

On the surface, the technology is very straightforward, but there are a number of very interesting features, limitations, and weaknesses of the systems that many users do not understand. Many of the statements in Information Week reflect a fundamental ignorance of what the technology can and cannot do. There are so many technical details about the systems that they cannot all be explored in a short case paper. For a detailed discussion of these we recommend (Molnar, 2004) and (Shutzberg, 2004). The most important of these are summarized in the following table.

Table 1. Technical Characteristics of RFID Systems

Frequency, Power, & Range	The range of a reader/tag pair is determined by the frequency of transmission and the power transmitted by the reader. The RF spectrum is tightly controlled and heavily used. In the US, RFID systems will operate in the 902 to 918 MHz range. In Europe the system will operate in the 862 to 870 MHz range. These frequencies support ranges around 20-30 feet. There are also short-range systems in the US operating at 13.56 MHz. This frequency limits range to 2 feet.
Interference from Materials and RF Devices	Devices are subject to many sources of interference. Readers typically cannot penetrate metals or liquids. Therefore, products containing these materials must be tagged and handled such that the material does not come between the reader and the tag. Interference also comes from other RF devices like bar code scanners, cordless phones, walkie-talkies, wireless networks, and security systems.
Multiple Reads	The RF wave from a reader triggers transmission in all tags within range. Therefore, a reader must contend with multiple simultaneous signals and multiple transmissions from each tag.
Accuracy of Reads	Wal-Mart's experience is that fully loaded pallets have a read rate of 66%, cases on stocking carts 90%, conveyor belts 95%, and trash compactors 98%.
Triangulation	Identifying the location of a specific tag requires triangulation from multiple readers that are placed in very specific patterns. A large number of readers are required to provide locations in a large area.
Speed of reading	Cases move through a Wal-Mart distribution center at 8 MPH. Readers must correctly identify a product at this pace.
Standard protocol, Frequencies, ID Codes	A number of standards in frequency, power, transmission encoding, data storage, and encryption are needed to make the systems work. Some of these are: ISO/IEC 18000 Part 6, ISO/IEC 15961 & 15962, ANSI INCITS 256:2001, EAN.UUC GTAG, ANSI MH10.8.4, and ISO 18185.

Hacking	Hackers can read tag data anywhere, anytime. For active tags, hackers may also be able to write and overwrite data on the tags. Encryption and reader verification schemes are under development.
Data fusion	In a tag-dense environment (like an Airbus A380), a reader will receive a large number of reads in a single scan. The will create a need for data fusion algorithms within the computers receiving the data.
Passive vs. Active	Passive and Active tagging systems present very different deployment issues. Active tags contain significantly more sophistication, data management, and security concerns.
Competing Tag Environments	Some environments will contain a number of tags from different manufacturers and systems. These may interfere with the operations of the native tags of the facility. Examples include USPS, UPS, FexEx and other sorting facilities.

Sources: Shutzberg, 2004; Molnar, 2004; Sliwa, 2005, Angeles, 2005.

This is just a summary of some of the more important technical issues. The references for this paper indicate that passive RFID is ready for deployment in wide public environment, but that active RFID systems present a number of issues that may prevent its public commercial deployment for some time.

Market Leaders

Given the huge potential of this technology, there has been a huge emergence of RFID specialty companies and the development of RFID practices within many market-leading companies. Several sources provided lists of these companies, but Shutzberg's was the most concise and well organized. It is reproduced here.

Table 2. RFID Market Leaders

Product/Service	**Companies**
Chips	IBM, Hitachi, Philips, AMI, TagSys, RFSaw, Charterate
Inserts	International Paper, MeadWestvaco, Texas Instruments, Avery Dennison, SmartTag, Rafsec, Power Paper, LabID
Printers	Zebra, Printronix, Alien tech, Intermec, Toshiba
Tags	Alien Tech, Matrics, Intermec, Philips, TI, SAMSys, MeadWestvaco, Flint Ink, Hitachi, Siemens, Power Paper, Avery Dennison, TagSys, RFSaw, Savi, Rafsec, FlexChip, Omron, iPico, Identec, Amatech, Tyco, Wavetrend, LadID
Antenna	Flint Ink, Avery Dennison, Moore, EMS, Omron
Readers	Alien Tech, Intermec, Matrics, Symbol, TI, SAMSys, Hitachi, Checkpoint, Savi, TagSys, Rafsec, Wavetrend, Feig, Omron, Tyco, Moba, Siemens, InKode, Amatech, Identec, iPico
Data Aggregation, Filtering Systems	IBM, OATSystems, ConnectTerra
Middleware	IBM, Accenture, OATSystems, Microsoft, SAP, Oracle, Sun, Savi,

	Wherenet, Checkpoint, Matrix, Sensormatic, Genesta
Directory Services	Verisign, Ember
Consulting	IBM, HP, Accenture, Bearingpoint, KPMG, PricewaterhouseCooper, Deloitte, Capgemini

Source: Shutzberg, 2004

Financial, Social, Legal, & Regulatory Issues

The most predominant issues to arise regarding RFID have been cost, privacy, and security.

The implementation of RFID systems will cost companies millions of dollars. These investments are usually driven by the demands of customers like Wal-Mart, while the hope that the system will reduce costs down the road must be taken as a matter of faith. However, most experts expect the technology to accomplish much more in terms of efficiency and cost savings than was achieved through the implementation of the Universal Product Code (UPC) nearly 20 years ago. Within many companies there is also hesitancy to allocate more resources for IT systems that are controlled by the CIO’s office. Every company has recently invested millions for new IT systems and is not necessarily prepared to continue directing their profits towards more IT. On the surface, RFID appears to be a production and distribution technology, but immediately beneath the surface is an ocean of IT systems for data collection, storage, analysis, and distribution.

Specific costs for the systems include tags, readers, tag printers, middleware, IT infrastructure, consulting, R&D, changes to internal business systems, training, third-party licensing, facilities changes, and labor (Shutzberg, 2004).

Many privacy organizations have begun a campaign to alert consumers to possible threats to their privacy. One of the most active of these has been CASPIAN, Consumers Against Supermarket Privacy Invasion and Numbers (McGinity, 2004). These organizations believe that a tagged product will be tracked as it leaves the store or library, but will be read again throughout the product’s lifetime. Anyone with a reader could potentially query passing pedestrians to determine where their clothes came from, what their spending habits might be, and what book titles are in their briefcase. Though this is conceptually true, it is much more problematic that it first appears. The technical limitations provided in a previous section illustrate the issues with read ranges, compatibility of devices, and interference from materials and multiple tags. For passive tags, it is also necessary to be connected to a huge database containing all of the product codes for the entire world. The perception of privacy invasion is much greater than the ability to realize it.

Organizations like CASPIAN extend their privacy objections from the world of the Universal Product Code (UPC), which they have been protesting for nearly twenty years. In spite of their opposition, the UPC is universally used within commerce and is probably a good indication of the degree to which RFID will be adopted. However, where the UPC is very useful for individual packages, the RFID will probably find a home at the case, pallet, and shipping container level. This means that UPC and RFID will co-exist for some time to come.

Since the devices are electronic, there is an opportunity to hack into the systems and read or change the data for some nefarious purpose. Passive tags do not allow the changing of data on the tag, so there is little opportunity to attack there. But it is possible to interfere with the reading of a tag from a near-by transmitter. The biggest threat is found in the use of active tags that allow an external device to read, write, and overwrite data in the tag. This opens the door for hackers to change the data in the tag or insert their own information for their own purposes. Molnar (2004) provides a great deal of detail about the vulnerabilities of active tags based on experiments with a library system using active RFID. Most recently, concerns of security have increased because a group of college students from Johns Hopkins University successfully hacked the RFID security system embedded in General Motors car keys (Schwartz, 2005).

Market Size

Analysts estimate that the RFID industry earned $300M in 2004 and they project a growth to $28B by 2009 (TechWeb, 2005). There are two big drivers of this expansion – the first is the adoption by major retailers like Wal-Mart and government agencies like the Department of Defense. The second is the reduction in the price of tags, readers, and IT systems required to deploy RFID. Currently, tags cost between fifteen cents and one hundred dollars. Many companies look forward to a drop in the tag price to five cents or less. The higher-priced tags are usually active tags with on-board power and more sophisticated electronics. These are most commonly used for very large products like automobiles, railroad cars, and high profit items like the latest fashions.

Strategic Positioning

In our opinion RFID systems will be widely deployed in the next decade. A number of the business areas are already flooded with strong competitors. These include the manufacture of RFID tags and readers, the development of middleware software for managing data, and consulting services on how to deploy the systems. Competitive positions are still available in printing, data aggregation, antennas, and directory services. The strongest players will be those who can capture large users like Wal-Mart and DoD. Companies who can create readers that are interoperable with US and European standards will have a strong position. We will also see the integration of RFID systems, Bluetooth, Palm devices, and cell phones. Companies that can bring all of these devices and services together will have a unique position in the industry. A wireless Palm Pilot or cell phone is a natural data access and alerting device for an RFID system. These take the data to a much wider audience than those holding a reader or manning a data collection terminal.

References:

Angeles, R. (Winter 2005). "RFID Technologies: Supply-chain applications and implementation issues". Information Systems Management.

Chabrow, E. (Jan 25, 2005). "Homeland security to test RFID tags at U.S. borders". Information Week.

Christenson, C. and Raynor, M. (2003). *The innovators solution: Creating and sustaining successful growth*. Boston: Harvard Business School Press.

Deloitte. (2004). "RFID:How Far, How Fast: A view from the rest of the world". Deloitte White Paper. Extracted from the Deloitte web site January, 28, 2005.

Deloitte. (2004). "Tag, Trace & Transform: Launching your RFID program". Deloitte White Paper. Extracted from the Deloitte web site January, 28, 2005.

Flint, D. (December 2004). "I've Got You Under my Skin!" Business Law Review.

Fusaro, R. (December 2004). "None of our business". Harvard Business Review.

Kanellos, M. (July 27, 2004). "Under-the-skin ID chips move toward US hospitals". c|net news.com.

Konkel, M; Leong, V; Ullmer, B; and Hu, C. (2004). "Tagaboo: A collaborative children's game based on wearable RFID technology". *ACM Journal of Ubiquitous Computing*, (2004) 8.

LaPedua, M. (Jan 25, 2005). "Radar golf claims breakthrough with RFID golf balls". Information Week.

Malykhina, E. (Jan 19, 2005). "Airbus delivers its RFID-enables, Next-generation aircraft". Information Week.

McGinty, M. (January 2004). "RFID: Is this game of tag fair?" *Communications of the ACM*. ACM: New York.

Meyer, P. (Jan-March, 2005). "When the Customer Says Jump". *Business & Economic Review*.

Molnar, D and Wagner, D. (October 2004). "Privacy and Security in Library RFID Issues, Practices, and Architectures". *Proceedings of the 2004 ACM Conference on Computer and Communication Security*. ACM: New York.

Ouellette, R. (2005). "On the nature of technology". Course Notes. University of Maryland University College.

Schwartz, J. (January 28, 2005). "Students find hole in car security system". New York Times.

Shutzberg, L. (October 2004). "Radio Frequency Identification (RFID) in the consumer goods supply chain". Industry White Paper. Rock-Tenn Company.

Sliwa, C. (January 24, 2005). "Retailers drag feet on RFID initiatives". ComputerWorld, 29(4).

Sullivan, L. (Jan 24, 2005). "Georgia court system hopes to trial RFID". Information Week.

TechWeb News. (Jan 12, 2005). "Sales of RFID tags forecast to rise quickly". Information Week.

Schwartz, J. (January 28, 2005). Students find hole in car security system. *New York Times.*