The State of RFID Implementation and Its Policy Implications: An IEEE-USA White Paper

15 April 2009

Introduction

This IEEE-USA white paper provides a basic introduction to RFID technology and the current state of its implementation.

Background

Radio Frequency Identification (RFID) is a form of automatic identification technology (auto ID). Auto ID is characterized by data forms that are machine readable. Other types of Auto ID include bar codes, magnetic stripes, optical character recognition, electronic article surveillance (EAS) security tags, optical character group (OCG) etc. These technologies can be further characterized by those that require contact in order to be read (magnetic stripes), and those that do not (such as, bar codes, EAS, OCG, RFID).

RFID differs from bar codes and most other contactless auto ID data forms in that the data can be read without a direct line of sight to the reader. Further, read distances can be relatively high (feet versus inches). Using RFID means that:

- Less human intervention is required in data retrieval
- Retrieval can be speedier
- With a properly installed and managed system, data captured via RFID is more reliable and obtained at lower costs

This higher degree of automation makes RFID poised to be an auto ID technology that could change the way data is collected and used.

Today, RFID is used in many applications, ranging from electronic payments to tracking goods through the supply chain. The use of RFID technology in closed-loop systems is as strong as applications for tracking goods. In 2008, the amount of RFID chips used in various closed-loop, mass transit tickets and cards was about equal to those used in open-supply chain goods tracking.

A SIMPLE EXAMPLE of a CLOSED LOOP SYSTEM

An example of a closed loop system is the disaster evacuation system for the State of Texas. The Texas National Guard, along with local jurisdictions, assists people requesting help in evacuating from a pending disaster (hurricanes are the common example). The efforts were historically effective, but planning for shelter, understanding the evacuation progress, knowing where individuals were located and being able to respond to concerned relatives required great effort including calling many shelters sites and hospitals to locate family members.

In 2008, Texas implemented a voluntary RFID-based Special Needs Evacuation Tracking System (SNETS), developed by Radiant RFID, LLC, to help manage the overall evacuation. Each person who requests assistance can opt to wear an RFID wristband. The wristband contains a unique number, bar code and electronic code that correlates to the person's personal data in a secure database. The wristband is read at evacuation bus boarding sites, transfer points, and final shelter locations. Friends and relatives can contact a 211 or 800 number printed on the band and request that the evacuee contact them. State officials then locate the evacuee in the SNETS database, and notify the evacuee of the inquiry. The wristband tracking system ensures the messages get to the right evacuation location's electronic message center, and allows return communications. The system does not disclose the evacuee's location (only the evacuee can divulge the location, within a message).

With the speed and reliability of RFID tag reads, this system is effective during the urgent pace of evacuating large numbers of people. More than 40 thousand wristbands were issued and deployed in 2008 for Hurricanes Ike and Gustav in Texas.

RFID Deployment and Concerns

Since RFID was first introduced in World War II to identify aircraft, the technology has improved as it has been implemented in a broad variety of uses, including identifying livestock and pets; shipping containers; managing vehicle fleets; increasing highway throughput; speeding up transactions at the point of sale; gaining entrance to buildings; real time asset tracking and mass transit ticketing. In the wake of 9/11, RFID is increasingly being used to enhance the authenticity of individual forms of identification, without creating longer ID authenticity verification wait times.

RFID is an enabling technology. Many varieties of RFID exist. Each needs to be verified independently. The technical and economic differences among the varieties dictate that decisions regarding the choice of users, including system integrators and other solution providers, hold the key to successful implementation of the technology.

RFID is not yet a plug-and-play commodity technology. Some providers will take a one-solution-fits-all approach, which invites complications and problems. Even when the optimum design is selected, it may need a custom design specific to the application to achieve optimum performance. Tradeoffs often need to be evaluated. For example, would the optimum performance of a more expensive custom design outweigh the economics of using an off-the-shelf design?

RFID underperforms in some applications because of a non-optimized solution approach. A basic understanding of RFID, its varieties, and custom design tools is important when evaluating its potential use in an auto ID project. Too often, the underlying engineering and physics are not understood, minimal training is provided, and expectations are unrealistic.

Consumer privacy and data security concerns are heightened by the longer read distances capable with RFID. The technology creates an opportunity for unsolicited RFID tag data modifications (reads/writes), and/or reads of which the tag carrier is unaware. This concern is somewhat unique to RFID forms of auto ID. Some varieties of RFID have built-in security protocols to ensure only authorized readers talk with only authentic tags. Most of these secure varieties also have technology design standards that limit data transaction distances to inches, versus feet, that minimize the threat of data hackers. Another aspect of security is whether to carry specific ID data on the tag (and entrust data security to the reader infrastructure), or to simply have the RFID tag contain a "license plate" that links to the real data held in a secure master data base. This decision is often made one application at a time. Standards and regulations for RFID technology rest with the industry to which the technology is being applied.

With a little imagination, fueled by sci-fi extrapolation, and a lack of rigorous analysis, another concern lurks. Some who espouse the danger of RFID-tagged products do so with an almost religious fervor. The fears of secretly being tracked are totally unrealistic, but security concerns are growing as RFID is being used in more personal id applications, such as credit cards and passports, as well as retail goods tagging.

Another concern is the security of proprietary data. How much does one company want to reveal to a competitor to gain efficiencies? That dilemma is of special concern in highly competitive industries, such as pharmaceuticals. Sharing data in an open supply chain means the manufacturer may have to share its pricing throughout the supply chain, including its competitors. Databases supporting open supply chain networks must be built with the understanding that some data must remain protected.

A final concern is the lack of global RF regulations regarding allowable frequencies, sideband ranges, and reader power levels. Given that our economy is global, that there is a lack of common regulations, and that the associated system performance produces substantial differences, engineering cost-effective solutions for the global open supply chain is difficult and complex. This lack of global standardization and regulation hinders the adoption of RFID as an open supply chain tool.

The point is that RFID technology has the ability to influence the supply chain, both positively and negatively. The ability to convey information digitally, during the entire life of goods and services, will cause a huge shift in the global supply chain operations and assist in ensuring authentic goods reach their destination. That a product can traverse the entire shipping and distribution network easily does not imply that the means to achieve it will be easy. We are just at the beginning of using the technology globally and ubiquitously.

How Does RFID Work?

RFID is essentially information carried by radio waves. The base technology comes from the fields of radio and radar engineering. Magnetic or electromagnetic fields are used for the data exchange between the RFID transponder and the reader and, in passive RFID varieties, are also used to provide the power supply to the RFID transponder.

The components of an RFID field are:

The **transponder** or **“tag”** is the data carrying element of an RFID system. RFID tag data capacity typically ranges from a few bits to several kilobytes. A tag typically consists of an electronic microchip and chip antennae designed to allow communications with a reader. In a “passive” system the tag is powered by coupling with the reader field. An active tag may be totally or partially powered via its own battery supply. Tags may be designed to be read-only or to read and accept writes.

Tags are typically packaged for the specific application. Tags may be embedded in a variety of materials, including paper, plastic cards, paper cards, injection molded plastics (such as key fobs), and glass (for use in a bodies such as animal identification).

The typical method used for sending data from the transponder back to the tag is backscatter, in which the frequency of the reflected wave correlates with the frequency of the transmission from the reader.

The transponder, or ‘tag’, consists of:

1. A microchip. These are now as small as 0.4mm by 0.4mm. Size is often a major factor in its price, since the smaller the chip, the greater the yield from a manufactured wafer. The wafer is processed by being grinded to final chip thickness, diced into individual chips, and then bumped for solder, wire, or flip chip attachment to an antennae. The chips are typically factory-programmed with an ID number during their contact testing phase. This pre-programming permits the use of the individual chip number in later stages of testing.
2. A chip antenna, designed for either magnetic or electromagnetic fields. The antenna is produced on a common substrate (e.g., PET). The antenna can be wires, etched aluminum, etched copper, or printed conductive silver ink, and a growing array of aluminum or copper antennae are being made with additive processes, such as electroplating. The antennae material does dictate certain performance characteristics, and one type may be more optimal in a given application. Wire antennae are often used in 125-134 kHz (lf) tags, as the high number of winding turns required at this frequency is easiest to achieve in a realistic footprint with small diameter wires.

An attachment process is used to secure the chip onto the antennae substrate and electrically connect the chip to the antennae. The chip bumping method, antennae material, and attachment process must be engineered together. After chip attachment, the inlay is RFID-functional and ready to be packaged.

Once the inlay is packaged into a paper ticket, label, plastic card, or other material, a final test is typically conducted on each unit, and non-conforming units are marked and sometimes removed. The testing also allows writing to be done to each chip in terms of a unique ID number. Programming of large data or object specific data, such as an electronic product code (EPC), is typically done near the end application (for example, with an RFID-enabled bar code printer systems).

The **reader** typically contains a radio frequency receiver and sometimes a transmitter, a control unit, and antennae to provide data retrieval or communication: It can be thought of as a digital communications system. A reader and/or chips can be designed to be Read-Only or Read-Write. Readers may also be designed with the capability to forward the received data to another system (e.g., via RS 232). The reader is used to provide commands to the tag, timing pulses and data, as well as coupled power for passive tags. It also receives data from the tag and must decipher this data relative to ambient RF noise. Most readers are designed to operate at a single channel or frequency. There are some designs that can read multiple protocols at different frequencies, but single channel frequency readers rule the day.

Reader system sizes range from the large fixed reader systems (size similar to shoplifting gates used in retail stores and libraries) that have the highest power (and thus the longest read distances), to the smaller mid powered readers, and even smaller handheld readers powered by batteries.

A unique feature of RFID is the ability to have multiple tags in the read field simultaneously. The system design feature that allows this is referred to as *anti-collision*. Anti-collision protocols are now part of many RFID standards, so that any vendor’s chip can work with any vendor’s reader when both are designed per a common set of standards. Anti-collision performance varies from reading a few tags per second to hundreds per second, depending on the frequency, the standard, and the amount of data on the chip to be read.

The reader antenna is important to the RF operation of the reader. Reader antennae designs can be made to maximize read distance, requiring tighter tolerances for the tag-to-reader coupling orientation, or they can be designed to be more robust to the tag-to-reader coupling orientation, but sacrifice some read distance.

The Federal Communications Commission (FCC) regulates the frequency and reader system RF emissions. RFID is operated at a shared frequency band, so care must be taken to prevent cross interference of RF systems sharing the same frequency band.

Software for RFID-derived data is typically designed to filter the large amounts of repetitive data capture inherent in many RFID systems. This filtered data is then used by application-specific host systems. Higher end readers may have data filtering capability designed in. The software may also act as a data verifier and require multiple tag reads at a given reader before accepting that tag as a legitimate.

Determining Read Range

Several variables have a major impact on read distances.

1. **Source of power**. Is the tag power derived solely from passive coupling, or is it entirely or partially powered by a tag battery? The typical maximum read distance of any passive system is in double-digit feet; the maximum for an active system is triple-digit feet.

2. **Regulated operating frequency**. The frequency of the system determines if the main operating principle is magnetic or electromagnetic. The frequency is also associated with the maximum regulated power that is allowable.

   Frequencies can be classified as follows:

   - LF (low frequency = 30KHz to 300KHz) magnetic
   - HF (high frequency = 3MHz—30MHz) magnetic
   - UHF (ultra high frequency = 300MHz-5.2GHz) electromagnetic

   The maximum read distances with magnetic based passive systems are in feet; the legal maximum read distances associated with passive electromagnetic systems are typically tens of feet.

   The field uniformity of the read field changes with the frequency. Higher frequency read fields tend to have more “holes,” or gaps in coverage, which is important to understand in detail.

3. **Type of microchip and its associated power consumption.** Some RFID chips may need fewer than 5 micro watts; some as many as 20.

   ♦ A simple read only chip with a unique ID only a few bits long is the most power efficient.

   ♦ A more complicated chip is a read-write-capable EEPROM (electronically erasable programmable read only memory). EEPROM requires increased power.

   ♦ An EEPROM chip with crypto logical functions to ensure authentic transactions has an even higher power demand.

   The highest power consumption chips have the most functionality, and can carry an operating system. These high-power chips are needed for financial transactions, as in contactless smart cards. These chips, which can support complex algorithms, are used for very secure data exchanges needing fast data communication rates. Generally, the more functionality required, the more power required, resulting in a design trade off. The trade off in a passive RFID system is between read distance and data transaction speed. Thus, high-speed data chips need a lot of power to work and the system is designed to trade off read distance for increased data speeds. These chips are typically practically limited to inches of read distance.

4. **Type of tag material**. The material that is placed on an RFID tag, or between it and the reader, will impact read distances. Especially with metals and water many materials have some impact. A tag can be designed for optimum performance on a given material, or tuned to work well enough on a wide variety of materials.

   A practical example is with high frequency tags used with library books. A tag specifically designed for hard-backed books with fine paper (e.g., encyclopedias) may get a 12-inch read distance on the kiosk checkout reader. The same tag put on a paperback book with lower quality paper may get a 9-inch read distance. A different tag tuning may be used to get 10 inches of read distance on either book type.[1]

The lesson from this example is that tag read distance needs to be measured by placing the tag on a typical object. Simply holding the tag up in the air is not a good test because the tag with the best read distance in free space may get the poorest result when attached to objects. Also, if multiple tags will be in the read field simultaneously, the maximum read distance will be less than if a single tag is read.

Under the principles of electromagnetic far field[2], an ultra high frequency (UHF) tag should obtain long read distances. However, it will use magnetic near field[3] principles for reads within about a wavelength (around one foot for 900MHz UHF). Also, the chip antennae are typically designed for electromagnetic operation, so their short read distance reliability may be poor. If the application will need both long and short distance reads,

[1] Countries mandate the use of different parts of the ISM band. For example, Japan, says UHF tags must transmit between 950 MHz to 956 MHz, while the European Union has specified the 865.6 MHz to 867.6 MHz range). Some manufacturers address these spectrum variances by tuning the tag to function best in specific parts of the spectrum. [http://www.rfidjournal.com/article/view/2156/1], Readers too are tuned in order to better receive the RF signal from the tag. Debuted a few years ago, some tags have microchips made with tunable transistors. A tunable transistor can self-correct for a range of variables such as deviations in the manufacturing process and changes in temperature **http://www.rfidjournal.com/article/articleview/799/1/13**.

[2] Far Field Communication -- In *Far Field Communication* the tag and interrogator antenna are coupled beyond one full wavelength of the carrier wave. The far field signal decays as the square of distance from the antenna, and is typically used in Ultra High Frequency and Microwave systems. Far Field Communication employs a backscatter radio link. [http://rfidsoup.pbwiki.com/Far+Field+Communication] Far field communication - RFID reader antennas emit electromagnetic radiation (radio waves). If an RFID tag is outside of one full wavelength of the reader, it is said to be in the "far field." If it is within one full wavelength away, it is said to be in the "near field." The far field signal decays as the square of the distance from the antenna, while the near field signal decays as the cube of distance from the antenna. So passive RFID systems that rely on far field communications (typically UHF and microwave systems) have a longer read range than those that use near field communications (typically low- and high-frequency systems). **http://www.rfidjournal.com/glossary/73**

[3] **Near-field communication:** RFID reader antennas emit electromagnetic radiation (radio waves). If an RFID tag is within full wavelength of the reader, it is sometimes said to be in the "near field" (as with many RFID terms, definitions are not precise). If it is more than the distance of one full wavelength away, it is said to be in the "far field." The near field signal decays as the cube of distance from the antenna, while the far field signal decays as the square of the distance from the antenna. So, passive RFID systems that rely on near-field communication (typically low- and high-frequency systems) have a shorter read range than those that use far field communication (UHF and microwave systems) **http://www.rfidjournal.com/article/glossary/3**

and you are using UHF tags, it is important to test the read reliability of a given tag at both long and short read distances.

Source of Tag Power

Tags can be passive, semi-active/battery-assist, or active tag. Active tags have battery, a longer read range and a transmitter that sends information to the reader. With a passive tag, data is sent to the reader by riding on the signal that is reflected back. (This is called backscatter.) Batteries are used to power the transmissions in active tags, but add significantly to the tag cost, size and limit the tag's life to the battery's life. Adding a battery, or additional power, to the tag means other energy-consuming components can be added to the RFID tag (such as sensors for temperature data logging for temperature sensitive products in the supply chain). These battery-powered tags result in more functionality but at an increased price. Active tags, when coupled with Global Positioning System, means tagged objects can be tracked in real time. (The U.S. military uses active tags to track container shipments.) Because active tags are expensive to manufacture and maintain, and passive tags are limited in distance and power, alternatives have been developed. Semi-passive tags, or battery-assist, tags use the battery to power the circuitry, but not the broadcast signal.

Active systems typically are based on prearranged times to" wake up" the tag to transmit to the reader. Passive and battery assist tags only transmit when close enough to the reader to couple enough power to transmit, and will then continue transmitting until moved farther from the reader.

Currently, the cost of a typical passive tag ranges from $0.11 to $1.00. (Generally, the higher the price the higher the power and longer the read distance.) Battery-assist tags cost $1.00 to $5.00, with a typical read distance of 100 to 200 feet, and active tags currently cost $8.00 to $100 and get up to 100's of feet of read distance.

Coding

The data stored in RFID tags depends on the application and existing standards. For example, the design of EPC global-supported code is divided into four sections (header, manager number, object class and serial number). Although many current RFID applications are based on proprietary systems, industries supporting open RFID systems with open standards may soon proliferate.

Some of the more widely used standards are as follows:

ISO 11784 and 1111785= ANIMAL ID

ISO 7810=CONTACTLESS SMART CARDS

ISO 10536= CLOSE COUPLED RFID

ISO 14443= HF PROXIMITY COUPLED RFID

ISO 15693= HF VICINITY COUPLED RFID

ISO 18000-PART 6C= UHF RFID

Issues

Recognizing that issues exist and improvements are being made to address the issues means we can avoid some of the problems that plague maturing technologies. However, this recognition requires an understanding of RFID fundamentals, so one can rationalize which changes will pertain to system needs, and to formulate the right questions regarding system testing, and fitness for use criteria.

Operation, testing, reliability, security, privacy, interoperability, data sharing, database use, and consumer confusion are the issues selected for this white paper.

Operation

Some current operational issues are as follows:

Mitigating Out-of-Sequence Tagged Unit Reads — Ideally, tagged items should be read in their physical sequence (e.g., in auto toll or conveyor belt). With RF, you can read an item early or late in its "physical order." With RFID auto-toll tags, this issue can be serious when the wrong person is billed. In logistical processes, such as a conveyer belt holding baggage, decisions are made automatically based on the tags read. If your bag gets read too early or too late, the mechanical switch sends the wrong bag to the wrong tray. Result: Bag is lost.

Conveyance Speeds vs. Tag Reads — Obviously, the faster the tag can be read, the better. Creating chips with larger data memory means more data to be read (requiring more time per read) plus higher chip power needs (lower read distance, which limits tag read time).

Reading Cases on a Pallet — Reading individual cases within a pallet is not a current requirement of most RFID systems, but it is the subject of much discussion – and expectations. Often, each box with a given material inside will interfere with reads. Tag placement on a box for any given material requires testing. Each situation is different. Some tags are specifically designed to overcome the problems caused by the laws of physics and material handling. Basically, you must test and select RFID tag placement areas on each box of a given material. Some materials are nearly impossible for some frequencies to pass through, so boxes in the inner stack of a pallet are the toughest to reliably read. The angle of the boxes to the read field (tag to read field coupling orientation) impacts read distance and thus read reliability. Depending on materials, reading all box tags on a pallet is currently not 100% robust for passive RFID.

Only when pallet-level tagging is improved will case-level and item-level tagging be seriously considered. A true supply chain application can only be achieved by placing products on shelves, so that the tags can be accurately read. Even a well-engineered item-level tracking shelf system can be defeated by the hurried shopper who returns an item to the shelf in a different position (for example, placing the item on its side vs. standing upright).

These problems highlight the needs of changing business practices in addition to manufacturing and distribution procedures

Determining Required Number of Antennae per Portal Type — The read zone of each reader antenna can “bleed” to another read zone, if the layout is not carefully calibrated. Also, higher frequency read fields tend to reflect off materials, so a tag may be energized and/or read by a reader that may not be the reader or portal closest to the tag.

Conflicting Applications — For example, the global airline industry is challenged by the RF interference generated by the metal bins that luggage is commonly transported in. The system must be able to distinguish between RFID tagging on airline parts and luggage, and there must be agreement on global procedures.

Ambient RF Noise — RF noise from other systems can cause read interference. A radio frequency noise site survey is typically done to determine reader placements, but few formal systems are in place to evaluate post RFID system installation and changes to equipment and their location, or to determine if older RF equipments’ shielding is breaking down. As RFID systems are increasingly used, these factors will need more attention. Another problem is when concentrated read points produces RF saturation to the point of being unreadable.

Testing

RFID has many flavors and, and each must be validated independently. This means that many different tests must be performed and is not a popular message because it will induce a lot of work. Test performance specialists observe that a need exists for globally recognized performance test specifications. Based on demand, standards-making bodies, along with manufacturers, are developing these specifications. However, applications have diverse needs and a generic seal of approval may be helpful, but certainly won’t address every RFID application or system. Test labs currently offer fitness-for-use testing to compare readers, tag designs, etc., in tests somewhat simulating actual system conditions.

Reliability

In many RFID systems, the reliability bar is high. Contactless credit card systems and global supply chain operations are two examples where the RFID network must be always on, reliable and secure, yet accessible. Until RFID reliability proves itself to be 99.99% reliable for an acceptable period of time, redundant system backups (e.g., magnetic stripes, bar codes, etc.) will be built into systems, such as magnetic stripes on contactless smart cards, bar codes on RFID supply labels, and license plate camera systems at RFID-enabled automobile toll stations.

Data synchronization is also an issue. Because there is no verification that the information is moving to the consuming application, the transaction queuing can produce unreliability in the data output.

Perhaps the biggest challenge to RFID system reliability is developing standard operating procedures. All successful RFID applications have implemented detailed procedures regarding RFID equipment installation, tag placement, process rules, etc. A great example is the concept of tag-and-go reader systems for contactless cards in mass transit systems. The cards have about a four-inch read range The tag-and-go procedure ensures reliable reads with a simple request to tap the card on the reader shell (fractions of an inch read distance). Therefore, a read is achieved despite any detuning impact of the user, or the tag-to-reader orientation. Like any system, all parts and procedures must work together and designed to avoid error, especially human error.

Certification

To validate accepted testing and reliability standards, a vendor-neutral body or bodies must be established and trusted to educate and certify RFID equipment, performance, system compatibility, etc. While all new equipment is made and tested to RF emission regulations, there is no preventive maintenance for recertifying equipment. Older equipment may emit higher levels of RF and cause interference issues.

A reader and its antennae are certified as a unit. If an organization plans to optimize the performance of in-house designed reader antennas, the system must be retested and certified. Always ensure the reader system is FCC certified.

While RFID systems may be certificated to operate legally, there currently is no good “housekeeping seal of approval” that applies to all forms of RFID relative to their stated performance and application suitability.

Security

The security framework must address

- authentication
- data protection and data system access control
- privacy from unsolicited read attempts
- unauthorized reading or writing to the tag
- use of the tag to track people movements.

Ensuring security is a stepped process, meaning that effective authentication, data protection, and control techniques cannot be embodied in one process.

Because there is little human intervention, the first step in establishing trust in the RFID process is determining authentication. That is, what is the process for two entities trying to communicate that guarantees they are who they say they are? Once the authentication process is complete, data is then moved to another system for authorization.

The RFID network is defined by the frequency, protocol, size of the antenna, the power strength in the tag and reader, and the distance between the tag and reader.

For a point-of-sale transaction, the tag remains with the product. At this point, the security issue is: Should the tag be deactivated to ensure privacy of the purchaser post-sale? If the tag remains active, restocking is easier in case of returns. Active tags can alert the consumer to date-sensitive products, as expiration dates approach. Deactivation programs could be similar to current loyalty card programs.

A study conducted by John Hopkins University and the security company RSA (JHU-RSA), “Security Analysis of a Cryptographically-Enabled RFID Device” (28 January 2005 Draft) [Source: www.rfidanalysis.org/DSTbreak.pdf] illustrates the problems and hype associated with the security of RFID data and use. As an example, the JHU-RSA team “cracked” the digital transponder encrypted challenge-response protocols of the popular Speedpass network that uses low frequency tags at the gas pump to accelerate the transaction of buying gas. As the researchers themselves acknowledged, the security was successfully challenged at only one level of a full Speedpass transaction. More recently, a Dutch teenager announced the cracking of popular Mifare HF-14443 encryption used on many mass transit tags.

While the ease with which the researchers and Dutch teenagers accomplished these breaches does raise concerns, personal and financial data are on separate networks, providing complexity and a buffer to unwanted breaches. The unique ID must traverse several computers for data lookups and authentication before traveling to off-site processing by an enterprise system, where it interacts with financial data that must be verified before the process at the pump can continue.

Regardless, the real-time nature of RFID data creates concerns for privacy and security experts. Eliminating paperwork and removing the human element may speed goods through the supply chain, but it also threatens traditional laws, regulations and procedures established to maintain the flow of goods across borders.

For competitive reasons, the last thing companies want to do is share their information with competitors. Companies sharing data in the RFID network must be confident the network and data are secure. To prevent radio snooping, a combination of authentication, encryption, and authorization is advisable. In addition to current systems for data exchange, authentication within the RFID system -- for example, between the reader and tag -- should occur before data is transmitted. Other measures to preserve privacy and counterfeiting can include encryption and the ability to deactivate a tag at the point of sale. But that makes the tag unavailable for after-market use. (Hargraves & Shafer, FTC, 2004)

Privacy

Privacy for consumers is like security for companies. To have data in the RFID network, one must be confident that the network and data are secure. In the privacy context, it is important to clearly (and perhaps often) communicate to users the distinctions among active, passive and semi-passive tags, along with their relevant range, cost and capability limitations.

For retailers, disabling, or “killing” product tags at checkout is still under discussion. In addition, the real privacy issue with RFID is not the limited data stored in the tags, but the security of the databases to which the tag data are linked -- a problem that exists today with minimal RFID implementation.

One argument against killing a tag is that, with RFID turned on, refunds and restocking returned items is quicker and more efficient than with current systems. As with customer loyalty programs, the customer should be able to choose between deactivating the tag and paying a higher cost, or accepting the tag as-is for a lower price. How the tag is deactivated, when, and under whose authority are still questions yet to be addressed satisfactorily. Complicating a global decision regarding a chip kill switch for applications in credit cards, passports, hospital wristbands, etc., where the accidental kill switch activation could result in problems for the user.

Regardless, deactivating the “always-on” RFID tag will remain a hot topic for the immediate future.

Interoperability

For the RFID network to provide the benefits that retailers like Wal-Mart determined for their return on investment strategy, RFID systems must be built for interoperability. Many trade groups, as well as vendors, favor systems built on open standards, which aid in building interoperable systems. For example, many UHF RFID tags are being built to meet standards developed both by ISO and EPCglobal (see **Appendix – Standards)**.

Labeling standards are less developed. Letting the general public know about the presence of an RFID tag in the box that was purchased is voluntary. For privacy advocates, acceptable practices, laws and regulations to enforce such practices are yet to be determined, although some governing bodies have attempted to pass laws barring the use of RFID in the name of privacy.

The unique identifier is the basis of the electronic product code (EPC) system and is a constant in all EPC specifications. Wal-Mart and the U.S. DOD proposed that eventually every item inventoried will be tagged by an RF identifier. Wal-Mart is requiring its 100 largest suppliers to comply or discontinue as a Wal-Mart vendor. As the world’s largest retailer, this dictum has significant global impact. Digital numeric identification -- manufacturers’ IDs, as well as electronic product object codes --comprises part of the data contained in an EPC tag.

Another issue of interoperability is global acceptance. RFID is spectrum-dependent, but countries vary in their use of spectrum. (See **Appendix E: RFID Frequencies per Country**.) For example, some RFID applications must manufacture systems using different frequencies, depending on the country where the system will be installed.

Interoperability for RFID will remain application specific for the immediate future. Thus, RFID credit card systems will be set up with readers and standards so any of the major credit cards and their chosen RFID chips can be read at any RFID-enabled credit card reader. These systems will have little in common with the Wal-Mart led open supply chain system; RFID enabled credit cards (HF/ISO 14443) are not readable on the EPC readers (UHF/ISO 18000 Part 6c) used in the retail open supply chain nor can the retail EPC tags be read on the RFID-enabled credit card readers and neither can be read at the RFID-enabled readers (HF/ISO 15693) at your local library. Note: ISO/IEC 18000-6c and EPCglobal Gen2 are similar and interoperable.

Electromagnetic Compatibility

Current regulations determine RF interference and RF safety levels on an individual device basis. For example, a TV remote control is regulated to operate at a frequency and power that will not interfere with any other nearby RF devices, and its RF emissions are at a level that presents no personnel safety risks. However, as more RF generating devices enter home and business ecosystems, it may become prudent to evaluate the cumulative RF generation in an area.

Another factor that may warrant evaluation is a time-based system to ensure that RF generating devices don't increase their RF emissions over time from factors such as RF shielding damage, etc. Currently, no inspections of RF devices are mandated, once they are installed in a system. Questions remain regarding RF inspection systems in various applications, such as in hospitals, private homes, or farm implementation.

Data Sharing, Database Use and Management

RFID systems in full-throttle, running 24/7, generate a lot of data. The proliferation of data, the sharing of the data, and the possibility of snooping via radio are all concerns. Developing and disseminating a policy framework for different RFID applications based on best practices and standards would help address legitimate concerns and enable deployment.

For example, the EPC does not describe the item or its owner, but provides a unique lookup identifier to databases that hold the information. Each datum itself, in its integral parts, is not a threat. It is when associations are built with accessed databases that sensitive relationships are revealed or discovered, resulting in damage -- actual or potential. To be able to decipher codes that protect and prevent access to RFID databases is daunting. With codes being standardized, it's only a matter of time before the program code to decipher EPC tag-data is widely available.

In addition, one of RFID's greatest strengths is to transparently connect supply chain trading partners to provide enhanced visibility across multiple points in the supply chain. This transparency requires the ability for information sharing across the supply chain network and the ability of network nodes to rapidly 'discover' RFID transactions and route them to the appropriate data consumers. Because RFID tag data is designed to have minimal intelligence, the network 'edge' must be able to collect, compile and publish this data and expose it to the appropriate consumers without violating any security or privacy concerns.

RFID can create mountains of information. Where will data be stored? How will it be managed? What archival procedures exist, if any? How will security and access be applied to the databases? With business leaning towards an easily programmable RFID network, how can RFID be introduced in a secure and controlled manner without compromising security? How will this network scale globally, and across the supply chain?

RFID readers could be used in attacks on personnel privacy via unauthorized reads of RFID tags. Should reader sales be regulated, licensed and registered? New products aimed at alerting an individual when they are in a RFID read zone are being invented, creating a solution somewhat akin to a radar detector. The individual can then decide whether the read is known and authorized, or is a potential security threat.

If using tags is going to be as common as bar codes, policies notifying consumers may also require giving the consumers options to permanently disable or discard the tags without incurring a cost or penalty. On the other hand, consumers may be enticed to leave the tags enabled, if the tags are integrated into their own personal network. For example, the “smart” refrigerator will be stocked with items that have their expiration date that can be “read” by the refrigerator or a handheld reader. Some home-based printers have integrated readers that won’t operate a given toner cartridge, unless it is verified as authentic by its RFID tag, so disabling the tag at the point of sale (POS) would make it unusable at the home-based printer. The printer companies adopted this solution to reduce grey market cartridges that were creating quality problems.

Consumer Confusion

Currently, each industry that uses RFID has mounted its own educational campaign to inform its customers about the technology. But RFID is a generic technology with many applications. Each application has its own benefits and limitations. One issue is how much is too much information for consumers. For example, the average consumer does not care about the technology behind the automobile industry’s use of read-only transponders that provide encrypted remote keyless entry. But they do care that the remote entry works all the time and is secure.

Acceptance of new technology takes time. Bar code technology, so common and accepted today, also had a long gestation period. Invented in the early 1950s, the first reader was installed in 1974 (Kahn, *Wall Street Journal*, 8 July 2005), roughly 20 years later. Today, bar coding allows many of us to scan and bag our own groceries to avoid long lines at the supermarket. Few small independent retail operators can survive without point-of-sale scanning equipment.

The real downside to consumer confusion is that it extends easily to policy-makers and law-makers, and is echoed in the press -- causing misunderstandings about the technology.

Conclusions

Evolving technology: Despite the relative age of RFID technology, any policies or technical developments must recognize that both RFID technology and its industry are currently evolving. Standards, too, are emerging, but none exist globally.

Openness and transparency: General agreement exists that the RFID network should be built on openness and transparency. Because RFID allows data to be collected inconspicuously, consumer organizations advocate clear notice of purpose, limiting data collection, and acceptance of accountability by business and consumers alike. Personal data privacy is of paramount concern. Security and privacy must be balanced against the limits of technology.

Data Transaction Security**:** Currently, the algorithms used to secure data transactions are not covered by standards.

An HF 14443b tag uses an open standard secure protocol. However, the security module and algorithm used in the reader and chip is not defined by the ISO 1443b standard. So, if you have a 14443b-based system and have a tag with a 14443b chip from vendor A and another from vendor B, you will not be able to read and write to both. Your reader will have a security module with the algorithm fore one or the other. The 14443b-compliant reader will read the unique chip ID numbers of either tag, but can only further read or write to the tag that the reader security module is compatible with.

Data Invasion**:** What chips should have kill features? U.S. citizens do not want any risk of killing the 10 year life of their RFID enabled passports for which $100 was paid, but may want the option of disabling tags on many items purchased through retail. Who should make such decisions regarding chip kill options?

Certification: A vendor-neutral means of certifying RFID equipment, systems, and specialists should be encouraged — especially because RFID technology is remotely readable, invisible and captures data in real time. Trusting that the data is being captured and transmitted safely and securely is valuable. Certifying that the RFID product is what is claimed and specialists are available to assist users, will be important to RFID technology proliferating.

APPENDIX -- RFID in Use

As a technology with boundless uses, here are some applications that currently garner management’s interest:

Retail

The cost savings and benefits of RFID in retail are associated with streamlining business processes, shipping faster, managing inventory better, and reducing labor costs. Wal-Mart’s expressed dedication to embracing the best that RFID can provide may shake up the doldrums for this retail giant. U.K.’s Tesco Corp. is tagging cases of nonfood items at its distribution centers for use in its stores. Target Corp. is requiring some suppliers to apply RFID tags to pallets and cases. At some point in the near future, the Food and Drug

Administration expects all pharmaceutical producers, wholesalers and retailers will thwart counterfeiting by placing RFID tags on pallets, cases and unit items.

Pharmaceutical / Healthcare

The desire to reduce hospital errors and healthcare costs has enticed many vendors and hospitals to work together, and may drive industry to use RFID tagging and tracking assets and even patients.

Airline baggage

Strapped with high oil prices and a glut of independent airlines, the airline industry is looking at any way possible to decrease operational costs. The average cost of misdirected or lost baggage can be as much as $200 per bag, according to industry analysts. Yet the cost-effectiveness of RFID is still marginal at best. Only a handful of airports use RFID in baggage tagging.

Airplane parts

Both Boeing and Airbus are using passive RFID tags to track and maintain airplane parts on their latest airplane designs. The U.S. Federal Aviation Administration authorized using passive RFID in this fashion, as long as the tags are not interrogated while the plane is in use.

Animal tagging

Tracking live animals from the farm, to food processing plants, and to a consumer’s table is of great interest to the food industry. Some producers and farmers actively support this investment; some fear it.

Passports

The U.S. Federal Government chose RFID technology to embed digital biometric data in passports. The capacity of the RFID chip for larger image files was one reason this technology was chosen over 2-D bar code already in use. The first generation chips contain all data, including the passport holder’s picture, readable on the passport data page. Data on the chip verifies the data page information, nullifying any illicit attempts to tamper with the passport. The U.S. State Department expects that future generations of the passport chip will contain fingerprint and iris images as well.

The International Civil Aeronautics Organization (ICAO), the *U.S. Patriot Act*, and the technology itself set forth the boundaries and requirements of the biometric passport. For example, ICAO requires the chip to contain a country-specific digital signature, so that when within range of the reader, this signature verifies that the government created the chip.

Auto tires

The U.S. Department of Transportation now requires tracking tires from the tire manufacturer to automobile manufacturers. Information about the plant, tire size and any unique attributes are spelled out in ANSI MH108.4 material handling specifications. More than 67 million new tires were shipped in 2000. In 2003, Michelin North America

Inc., implanted RFID tags on some tires to keep track of their performance and wear. Dealers and service centers can better track inventory and determine tire performance.

Libraries

The thought of being able to check out books without a librarian's help, of the library completing a comprehensive inventory in record time, and easing the burdens of repetitive tasks of checking in a book have made RFID applications in the library very attractive, and a fast-growing RFID application. To maintain user privacy for this item-level application, organizations such as the Electronic Frontier Foundation advocate practices like private authentication (see Libraries in Appendix – Standards).

Supply chain

Theft, counterfeiting, terrorism, transportation and product diversion are all major concerns in delivering goods. The costs associated with them inevitably add to the cost of goods sold.

Any organization within the supply chain encounters:

- Incorrect goods shipped
- Late delivery of goods
- Difficulty locating goods
- Difficulty reconciling physical goods to customer orders/returns
- Misplaced/stolen goods
- Inaccurate forecast of goods

Appendix-Standards

Especially for one of the major intended uses in the supply chain and logistics, RFID must be based on global, non-proprietary, royalty-free standards. Suppliers are working on interoperable protocols now dependent on radio frequency, distance, power and reading speed. Standards required fall into five categories:

Air interface protocol (communication between tag and reader)

Data content (organization and data format)

Conformance (testing)

Applications

Packaging

ISO Standards

Currently, RFID tagging uses the International Organization for Standardization (ISO) standards.

EPCglobal Standards

Standards developed for the electronic product code (EPC) evolved from those proposed by the Auto-ID Center. To track products through the supply chain, the Auto-ID Center was established in 1999. Initially rejecting ISO standards as too complex, the Center established electronic product codes to be used much like the bar code is now. Because the EPC had to be readable in an environment requiring a longer read range, the standards were developed for ultra-high frequency, along with network architecture to support web-based tracking. The Uniform Code Council (UCC), which oversees bar coding standards, licensed the EPC technology and formed EPCglobal, a joint venture with EAN International, formerly AutoID, Inc. EPC codes are similar in structure to those standardized under EAN. Class 0 and Class 1 standards are now in use.

Generally, spectrum for lower frequency tags is available globally. However, UHF spectrum is not universally available. Although EPCglobal Generation 2 standards may offer forward compatibility, ISO and EPC standards currently are incompatible. Systems based on Gen 2 standards are due out later this year from many manufacturers. Many of them also worked on the ISO UHF standard, in the ISO 18000 series. Gen 2 tagging is faster, more secure, and feature rich. Gen 2 has a longer range than Gen 1, Class 0, and 1, and it avoids interference.

International Civil Aeronautics Organization (ICAO)

Draft standards for biometric passports were released December 2004, relying on ISO 14443. See: www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

IEEE, ISO/IEC, ECMA International, ETSI, and several national standardization bodies are working for the adoption of global standards for RFID.

Data Structure

For RFID to be as pervasive as the business community projects, global standards for handling data must be accepted and used universally. Users and businesses should have clear intentions about who controls what data in the supply chain. For example, consumers should be able to control the use of data and identity information. No one business should have all the data used throughout the supply chain. Control over data and personal privacy govern RFID’s acceptance. Information practices differ, depending on region and culture, but the elements of importance are as follows:

- Notice. Open and transparent information collection.
- Declaring intent. Collection of personal data relevant to the purposes for which it is collected.
- Limited use. Use is only for the intended purpose.
- Accurate. Collected data is accurate, complete and timely.

- Protected. Personal data is protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification, or disclosure.
- Access. Individuals can view all information collected about them.
- Accountability. Compliance to these elements is implementable.

IEEE

802.11

802.15.4. The standard for wireless personal networking is the basis for the Zigbee, high-level protocols for low-power, digital radios. Membership in the Zigbee Alliance is required for commercial use. Meter reading is one such application.

1902.1 RuBee

Proprietary Standards

Zigbee [Source: www.mywiseowl.com/articles/ZigBee]

Government

U.S. Government RFID applications are summarized in the following table.

Department of Defense (DOD) RFID Tagging Policy

The following is a high level view of DOD's tagging policy. By January 2007, the EPCglobal tag data construct will comply with the Department of Defense's Commercial and Government Entity (CAGE) code, and the DOD's Activity Address Code (DODAAC) -- used by suppliers to identify shipments.

Federal Communications Commission

In the United States, the regulation of RFID falls largely to the FCC, since it regulates allowable frequencies, power output, emissions and other performance characteristics (FCC Title 47, Part 15). For example, the 2.4 GHz and 902-928 MHz frequency range is identified for industrial-scientific-medical and short-range devices. Because the FCC oversees the combination of frequency and allowable power levels, the functional range, such as the power output of a reader, is also under FCC's purview.

> "RFID is regulated under Part 15 of the FCC's rules for low-power devices. Since Part 15 equipment has a relatively low probability of causing harmful interference to other wireless operations, a user may operate it without a license. Although RFID devices are unlicensed, the FCC's rules require that (with limited exceptions), they must be authorized by the FCC as meeting its radio frequency (RF) emissions limitations, power restrictions and other requirements before they may be operated or marketed." (Quirk, *RFID Journal*, 11 April 2005)

Federal Trade Commission

The FTC has a vested interest since the technology and its devices facilitate many of the activities that involve consumers. In its June 2004 Radio Frequency Identification Workshop, the FTC was the first government agency to begin public dialog about RFID. [See: www.ftc.gov/bcp/workshops/rfid/index.htm]

Department of Health and Human Services/Federal Drug Administration (DHHS/FDA)

The DHHS/FDA regulates the pharmaceutical industry, which is seen to benefit from RFID, especially as a defense against counterfeit drugs. FDA released guidance in its November 2004, *Division of Compliance Policy*. Injectable devices -- for both animals and humans -- are also under study, as well as adhesive tags for humans.

To date, the FDA has issued no more than a few reports and guidelines. However, it is relying on stakeholders, such as pharmaceutical companies, to use RFID technology to help eliminate counterfeiting. This government agency will have to be a principle player in determining how and what labeling will apply to incorporate RFID tagging. To date, only unenforceable guidelines have been issued.

As with wireless devices, issues about electromagnetic compatibility of RFID tags remain to be identified and resolved. For example, the stability of susceptible drugs exposed to electromagnetic radiation associated with RFID and interference with other devices has yet to be determined. Devices possibly susceptible to picking up signal harmonics include neuro-stimulators and pacemakers.

Department of Commerce/National Institute of Standards and Technology

In addition to the general role that the DOC has in overseeing U.S. commercial interests globally, it's the home for NIST. The agency's mission is to "develop and promote measurement, and technology to enhance productivity, facilitate trade, and improve the quality of life." DOC recently hosted an RFID workshop on RFID that coincided with its publication of a six-month study on RFID.

U.S. State Department

The State Department plans partial issue of passports with RFID tags beginning in late 2005 as part of its goal to prevent passport fraud, with full implementation by October 2006. To date, privacy and security advocates have assailed the use of RFID in passports. Framed by requirements of the ICAO and the *U.S. Patriot Act*, and in conjunction with the Department of Homeland Security, the State Department is required to complete roll out of biometric passports by FY 2008. In the meantime, it is addressing all issues raised by citizens, interest groups and regulatory bodies. In addition, a less expensive passport for North American border crossings only was released in 2008. This passport uses the passport as an Easy Pass Toll Tool at border crossing. It is a long read distance passive tag. The passport contains a unique number that correlates with a security profile in a secure government data base and gives the border agent a green or red light on your profile.

Appendix C - Typical Tag Types

Type frequency	Frequency range	Read range	Memory	Comments
Microwave	2.45 GHz	2 meters max	Less than 1 Kbit	Silicon technology is in its infancy for this frequency. Not expected to change any time soon.
Ultra High Frequency	300 MHz to 3 GHz (typically 866 to 960 MHz; 915 in the U.S.)	As much as 6 meters or more, depending on regulatory requirements (4 watt EIRP in the US; 2 watt ERP in Europe)	1 Kbit for now, larger expected in near future	Sends faster and further than lower frequencies, with good anti-collision capability. Not yet available globally, since spectrum use varies with country. (Europe uses 868 MHz for UHF; the U.S. uses 915 MHz. Japan prohibits the use of UHF spectrum for RFID, but may open the 960MHz area.)
High Frequency /ISO 16593 (vicinity smart cards)	3 to 30 MHz (usually 13.56 MHz)	1.5 meters at best for high-end readers	256 bit to 8x32 bit blocks, 4kByte additional data memory available today	Inductive nature of coupling between tag and reader (near-field coupling) prohibits larger read ranges, even for increased field strengths. Antennas for tags usually consist of printed, flexible coils that make the technology ideal for smart cards.
Low Frequency	30 kHz to 300 kHz	1 meter at best	64 bits to 1360 bits, larger possible but customers prefer 13.56 MHz instead	Globally available frequency. Low frequency allows tags to be read through watery substances, the only technology that allows for this capability. Low frequency does not allow for fast dataspeeds though, which is the reason

that (as a rule of thumb) no anti-collision handling is offered for tags using this frequency. This technology is also the only one that allows for small ferrite-based coils as tag antennas, which allow for a small cylindrical form factor for the tag — an advantage in many RFID applications.

Appendix D - RFID Frequencies per Country

Frequency	**Regions/Countries**
125-134 kHz	United States, Canada, Japan and Europe
13.56 MHz	United States, Canada, Japan and Europe
433.05-434.79 MHz	In most of Europe, United States (active tags at certain locations must be registered with the FCC), and under consideration in Japan
865-868 MHz	Europe
866-869 and 923-925 MHz	South Korea
902-928 MHz	United States
952-954 MHz	Japan (for passive tags starting in 2005)
2400-2500 and 5.725-5.875 GHz	United States, Canada, Japan and Europe

Appendix E - 2009 IEEE-USA CCP Membership Roster

Officers:
Doug Taggart, Chair
Eric Burger, Vice Chair

IEEE-USA Staff:
Deborah Rudolph

IEEE Society Members:
Jean Camp, Society on the Social Implications of Technology
Jack Cole, Computer Society
William T. Hayes, IEEE Broadcast Technology Society
John Healy, Reliability Society
Ferdo Ivanek, Microwave Theory & Techniques Society
Stanley Klein, Power & Energy Society
Stuart Lipoff, Consumer Electronics Society
Wayne C. Luplow, Consumer Electronics Society
Luke Maki, Professional Communication Society
Dhawal Moghe, IEEE Region 5
John Newbury, Power & Energy Society
Tirumale Ramesh, IEEE Region 2
Curtis Siller, Communications Society
Wesley Snyder, Robotics & Automation Society
Emily Sopensky, Intelligent Transportation Systems Society
Erdem Topsakal, Engineering in Medicine & Biology Society

Members:
Michael Andrews
Jay Greenberg
George Mattathil
Robert Powers
John Richardson
Paul L. Rinaldo
Carl R. Stevenson

Corresponding Members:
Stacey Banks
Thomas Cylkowski
Hillary Elmore
Matthew Ezovski
Ann Ferriter
Jon Garruba
David Kunkee
Richard Lamb
Philip Olamigoke
Wayne Pauley
Norm Schneidewind

Resource Members:
Michael Marcus
Mike Nelson

2009 UPDATE

TABLE OF CONTENTS

This publication revises the 2005 white paper developed by the IEEE-USA Committee on Communications Policy (CCP), with special assistance from CCP members Emily Sopensky and Peter Kuzma.

IEEE-USA
2001 L Street, NW, Suite 700
Washington, D.C. 20036
+1 202 785 0017
+1 202 785 0835 fax
Web: http://www.ieeeusa.org
POC: Deborah Rudolph
E-mail: d.rudolph@ieee.org