International Journal of Innovation, Management and Technology, Vol. 1, No. 2, June 2010
ISSN: 2010-0248

RFID – The Best Technology in Supply Chain Management

Kamaladevi B

Abstract—**During the last decade, most organizations have implemented enterprise-wide applications and integration platforms. These implementations have delivered benefits in terms of data synchronization and information flows within the organization, and with trading partners providing valuable inputs for planning and optimization of schedules and reporting. However, automated data capture and tracking in real-time has been a major bottleneck, affecting the ability of organizations to optimize their investments in supply chain solutions.**

Radio Frequency Identification (RFID) Technology is emerging as a technology that could provide the answer to these problems. Using tags, readers and radio waves to communicate between the two, RFID combined with the EPC (Electronic Product Code) would be able to address these pain points and deliver a whole range of benefits across various verticals like manufacturing, distribution, retail, logistics, and security. The potential benefits arise from increase in supply chain visibility, increase in efficiencies and decrease in costs due to better data synchroni\zation, increase in responsiveness to changes due to real time information visibility and a number of additional industry / vertical specific benefits. RFID promises to have a major impact on supply chains allowing trading partners to collaborate more effectively and achieve new levels of efficiency and responsiveness.

This paper describes technical research on the problems of privacy and security for RFID and also explores solution for privacy and security problems using Five Phase Life Cycle Model.

Index Terms—**RFID Technology, Supply Chain Management, Privacy, Security, Electronic Product Code**

I. Introduction

An essential ingredient for an effective and efficiently managed supply chain includes accurate, real-time information about products within the chain. The integration of RFID systems within a company's supply chain offers an abundance of economic and productive capabilities. An RFID is a "white" tag with an imbedded microchip containing product information which can be accessed by a receiver using radio frequencies. The "white" tag is affixed to the product at the pallet level while still at the warehouse prior to shipment.

Companies such as GAP, CVS, Gillette, Proctor & Gamble and Wal-Mart have recognized the importance of leveraging RFID technology to improve and increase operating efficiencies in the supply chain, which is benefiting from recent advances in electronic cataloguing. With RFID systems, companies would have increased product visibility, reduce out-of-stock items, trim warehouse costs, eliminate stock errors, reduce theft and shrinkage and allow companies to regularly update their logistics and inventory databases. Several pilot studies are underway globally to study RFID system application and its integration within existing ERP systems. Most companies are taking a cautious approach and initially focusing their study of RFIDs at the pallet level before progressing towards each product unit stored in a box.

RFID is the latest magic bulletin in the technological scope that has the potential to make a sweeping shift in the way any organizations approach their supply chain. Leading the way in embracing this technology are retailers, particularly Wal-Mart and their suppliers. RFID is enabling companies to see further into the supply chain than ever before, providing more accurate real-time information and improvements in process efficiency. The increased visibility can result in faster inventory turns, less shrinkage, reduced labour and higher material flow through warehouse or distribution center. Greater efficiency means RFID-enabled processes take less time and effort; entire pallets of product can be recognized in seconds without the need to break them down, and cycle counting inventory can be accomplished in hours or even minutes instead of days. RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years-and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers.

II. Review Of Literature

Juels' survey gives a good introduction and overview on some of the central topics in RFID security. Lehtonen et al. limit the scope of their examination to product authentication and a discussion of the trade-off between complexity and security in different RFID authentication methods. Moreover, there are publications on state-of-the art in RFID privacy preservation, as well as numerous reviews on security and privacy concerning health care, e-commerce and data mining. The latter two are especially interesting, as essential privacy questions in these fields, like "What data is collected?" and "How is data secured during transmission?" apply to RFID as well. The central factor underlying these topics in e-commerce is trust, a topic that can easily be anticipated in an RFID context. When RFID tagged objects hit the end-user

B.Com, DTE, DECT, MBA, PGDPMIR, PGDRM, M.Phil Student, Dravidian University, Kuppam, Andhra Pradesh, India.(email: kamaladevimba@gmail.com).

market at a large scale, consumers' willingness to provide data will likely depend on individual perceptions of trustworthiness, just as it does in e-commerce. Such perceptions will be directly based on the security and privacy provided.

Due to the invasive nature of RFID tags many privacy issues and concerns exist. An issue that moves to the forefront with the use of RFID tags deal with tracing and tracking of RFID tags. The tracing and tracking of data from tagged objects in the supply chain by competitors poses the threat of corporate espionage (Garfinkel, Juels et al. 2005). Tracing and tracking of data after the sale poses consumer privacy issues as tags can be well hidden in packaging (Ayoade 2007). Additionally, RFID tags respond to interrogation request from all readers allowing data to be gathered by others external to the organization (Juels 2006).

There are many methods for disabling RFID tags and preventing data from being visible that are currently in use. Additional methods have been proposed for rendering RFID tags inoperable. Implementation of devices and methods such as blocking tags, clipping tags, soft blocking tags, selective blocking tags, and kill commands are used to block or impede the propagation of the RFID signals. Blocking tags are special devices/tags that interfere with the protocol that is used for communication between normal identification tags and readers (Ayoade 2007) and (Jules and Weis 2006). Tag clipping involves disabling the RFID device by removing or breaking the connection between the chip and the antenna. Günter Karjoth and Paul Moskowitz identify several methods to effectively clip tags through the use of tags with removable electrical conductors, the use of tags with perforations, and the use of tags with a peel-off layer (Karjoth and Moskowitz 2005). Soft blocking is a variation on the blocking concept that operates through the utilization of software or firmware. Soft blocking provides for the possibility of utilizing privacy protocols (Juels and Brainard 2004). Selective blocking tags involve altering a blocker tag to prevent the transmissions of a selected set of tags (Juels, Rivest et al. 2003). The kill command is a method of permanently disabling an RFID tag as the tag moves into the hands of a private owner (Juels, Rivest et al. 2003).

Radio frequency identification security as defined by Ranasinghe, Engels, and Cole is composed of the following components; confidentiality or message content security, integrity of message content, authentication of sender and recipient non-repudiation by the sender, and availability (Ranasinghe, Engels et al. 2004). However, this study will discuss security based upon the following criteria – vulnerabilities, protocols, and cryptography.

III. Theoretical Background

Are the supply chains working at 100% or even 90% expected levels? Not quite. The reasons for this are varied, let's see the reasons and their **impact:**

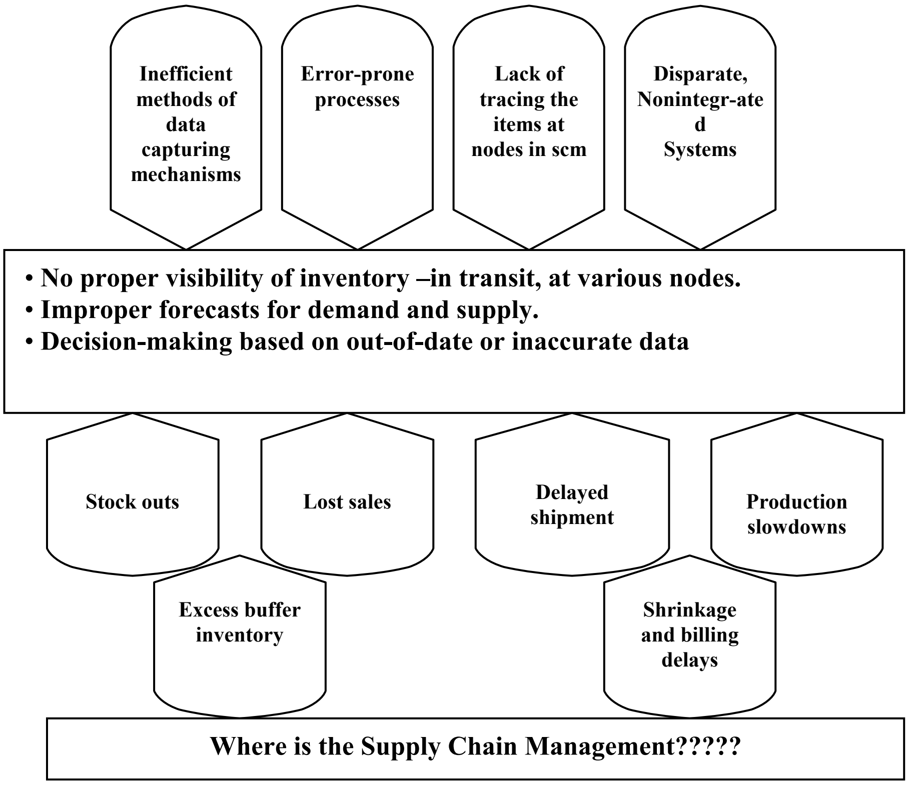
Inefficient methods of data capturing mechanisms
Error-prone processes
Lack of tracing the items at nodes in scm
Disparate, Nonintegr-ate d Systems
• No proper visibility of inventory –in transit, at various nodes.
• Improper forecasts for demand and supply.
• Decision-making based on out-of-date or inaccurate data
Stock outs
Lost sales
Delayed shipment
Production slowdowns
Excess buffer inventory
Shrinkage and billing delays
Where is the Supply Chain Management?????

Chart No.3.1 Where is SCM?

The problem can be put in better perspective with respect to retail environment where there are almost lakhs of SKU's to be handled. The problem of stock-outs has a high negative impact on the top-line as well as bottom-line, according to a survey carried out by HBR. The survey had a sample size of 71,000 respondents in around 29 countries. This survey indicates some of the fears the retailers and companies managing different brands have with regards to consumer buying behavior. The survey was about what happens when consumers can't find the precise product they're looking for?

The most important finding of the survey suggests that retailers could loose nearly half of intended purchases when faced with stock outs. For a company like Wal-Mart this could mean 4% of the sales. That's a staggering 8.5 Billions by Wal-Mart's current size. Excess production seems to be

the obvious solution but it may have some horrendous effects on any firm because of highly decreasing product life cycle where the factor of obsolesce is very high.

"Problems cannot be solved by thinking within the framework in which the problems were created"

- Albert Einstein

What is needed is an effective solution for end to end visibility that places the right amount of goods at the right place and in the most cost effective manner. There is an urgent need for businesses to "Sense and respond" which in turn requires every vital part of the enterprise to be integrated with the IT infrastructure, and this has to include the physical assets (inventory, equipment, infrastructure etc.) but most importantly enable *item-level tracking*. This calls for the ability to give electronic identities to passive objects, bringing them on-line. One of the ways is with the help of bar codes. Bar codes, the most primitive form of tagging, were all posed to bring the revolution in the era of 1980's. Using barcodes, information about an item can be captured using optical barcode scanners. However barcodes have a number of limitations.

The future is smaller but smarter--- *Welcome to the World of RFIDs*

RFID is a type of auto ID technology that uses radio waves (as the name Radio Frequency Identification denotes) to identify, monitor and manage individual objects as they move between physical locations. So, RFID is a smart sensing technology. The RFID Technology has been compared with the existing and well-established competing Bar-coding Technology.

IV. Research Methodology

The objectives of this research are two-fold:

1) To analyze the problems of privacy and security for RFID
2) To give solutions for privacy and security problems using Five Phase Life Cycle Model

A descriptive research design suits for this type of research. Case study method is used for analyzing the objective. More than that, personal interview was made with the managers and customers of the shopping malls like Central, Forum, Globus, Big bazaar in Bangalore. This interview gives an idea about the practicality of RFID. Based on the idea, this paper is analyzed about the problems of privacy and security considerations for RFID and also to explore solutions for privacy and security problems using Five Phase Life Cycle Model.

V. Privacy & Security Considerations

Privacy considerations are interrelated with security considerations. A key objective of any RFID security program is to identify risks and controls for safeguarding personally identifiable information (PII). An organization implementing a security and privacy program for an RFID system should consult its privacy officer and legal counsel throughout the information system development life cycle.

A privacy program may protect different types of personal information. Some information is personally identifiable, meaning that someone can use it to identify a particular individual. Other information may not be personally identifiable, but individuals may still consider it private even in settings where they are anonymous. For example, an individual anonymously traveling on a public bus may not want other passengers to know what items are in her handbag. Information that is not PII typically is not subject to legal requirements, but many people may still consider this information personal and worthy of safeguards. Therefore, organizations may still choose to implement privacy controls voluntarily to safeguard information its customers, business partners, employees, and other stakeholders consider personal.

Federal law governs Federal government agencies' collection and handling of PII. Relevant statutes include the Privacy Act of 1974, the E-Government Act of 2002, FISMA, and the Consolidated Appropriations Act of 2005. OMB memoranda provide policy guidance and instructions for agencies' implementation of these laws. The privacy of health information is covered by HIPAA, which applies to non-Federal as well as Federal entities. The Federal CIO Council developed a list of privacy control families that provide a reference framework for those integrating privacy principles into RFID systems. In some cases, controls can serve to enhance both security and privacy. In other cases, the privacy controls complement security controls. Since RFID implementations are typically highly customized, the privacy controls listed are not always applicable or may not be effective for all RFID systems.

VI. The Applicability Of Privacy & Security Considerations To Rfid Systems

RFID systems support a large variety of business processes, not all of which involve personal privacy. Examples of RFID systems that likely do not have privacy considerations include those supporting industrial processes, animal tracking, and asset management systems in which the assets are never associated with individuals during their life cycle. Privacy considerations exist when the system uses, collects, stores, or discloses personal information. An RFID system might use or disclose personal information in one of several ways:

1) Personal information such as a name or account number may be stored on the tag or in a database in the enterprise subsystem.
2) A tag may be associated with a personal item such as a bottle of prescription medicine, or a folder of legal documents that might be outside of the individual's possession.
3) A tag may be associated with an item that often travels

with an individual, such as a tagged box or a vehicle part in an automobile or truck the individual often drives.

The RFID system does not have to store personal information to have privacy implications. For example, the tag on a bottle of prescription medicine may identify the drug in the bottle, but not the identity of the person for whom the prescription was written. Nonetheless, the individual taking the medicine may still perceive the possession of the drug as personal information if scanned and read by another, as it might reveal information about a medical condition that the individual considers private.

Similarly, the individual does not have to own a tagged item for the RFID system to have privacy implications. For example, if an employee carries an employer-tagged computer or tools, then RFID technology potentially could be used to track the employee's whereabouts. The employee may agree to be on-call after business hours but could consider his or her location during those times as personal information.

While the concepts of privacy and PII are not new, RFID technology is an example of a technology that introduces new complexity to the landscape of privacy considerations for several reasons. For example, RFID technology increases the likelihood that someone can create PII through indirect means. RFID technology creates opportunities to record, store, and process item-specific information related to business transactions more easily than ever before. In addition, the breadth of items in everyday life that will be incorporated into RFID systems is expected to increase in the coming years. The increase in the coverage of information systems in our daily life combined with the increase of the level of detail of information in those systems will likely create new opportunities for combining data elements to generate PII. Advances in Internet search and data mining software also will facilitate the ability to capture PII from large volumes of what previously might have been considered uncorrelated data. All of these trends can occur even if PII is not recorded on tags themselves.

Several inherent features of RFID tags make enforcement of privacy controls more difficult than traditional information technology systems. Organizations may face challenges enforcing privacy policies when they cannot be coupled with effective security controls. RFID uses wireless communication, which is more vulnerable to eavesdropping and other attacks than the wired systems on which most traditional IT systems reside. In many applications, RFID tags will travel between organizations and often will be found in public areas, which means they cannot benefit from physical security commonly provided to most traditional IT systems. In general, RFID computing resources are limited and are not capable of implementing sophisticated technical controls. As this document describes, many techniques exist to mitigate these security and privacy risks, and these are expected to improve over time. However, the economics of many RFID applications will require low cost tags with limited functionality, which has significant implications for privacy protections. Finally, in many applications, especially those involving passive tags, identifiers can live beyond the usefulness of the application for which they were intended, but still may store PII or be used to generate PII when combined with other data. While traditional IT systems have well-established policies and procedures for the retention and destruction of data, destroying or disabling tags may be infeasible once they are outside the control of the organization managing the RFID system.

RFID technology may introduce new privacy considerations that are not fully understood today. Privacy regulation and principles evolve to meet the demands of new IT systems. For instance, technical advances such as the Internet, electronic databases, and analytic system software have made the collection and sharing of PII easier than it was in a world of paper files. RFID technology further extends the reach of IT systems and the collection and sharing of information that might be considered personal. While today RFID readers typically are located in designated locations to support a particular business process, in the future readers may be ubiquitous and capable of supporting multiple objectives. For example, today an RFID system might be implemented to provide access control to a facility using RFID-enabled badges. Badge holders are unlikely to possess other tagged items. In the future, badge holders may routinely carry a number of tagged items, and the badge reader may be used to scan them and create a profile as well as authenticate the badge. The data collected might be shared with third parties for justifiable business needs and with legitimate data sharing agreements. The systems might be implemented with disclosure and consent, but may not be effective because individuals and organizations cannot reasonably understand all the potential uses of the data or predict what type of transactions might create PII through indirect inference. For these reasons, new privacy tools and concepts may need to be developed to address the complexity introduced by RFID technology.

VII. Solutions For RFID Problems Using Five-Phase Life Cycle Model

RFID systems typically must be highly customized to support the business processes they automate; no one-size-fits-all approach will work across implementations. Nevertheless, organizations can benefit from following some general principles when using RFID technology. It describes a set of recommended security practices that can help organizations manage RFID risks to an acceptable level.

To be most effective, RFID security controls should be incorporated throughout the entire life cycle – from policy development to operations. The five-phase life cycle helps organization to determine the most appropriate actions to take at each point in the development of the RFID system. The phases of the life cycle are as follows:

Phase 1: Initiation

This phase covers the tasks that an organization should perform before it starts to design its RFID system. These tasks include conducting a risk assessment and developing policy and requirements with which the RFID system must comply.

Phase 2: Acquisition/Development

For the purposes of this guide, the acquisition/development phase is split into two sub-phases:

Phase 2a: Planning and Design

In this phase, RFID network architects specify the standards with which the RFID system must comply, the network infrastructure that will support the system, and the technical characteristics of the RFID system, including the types of tag and readers that will be deployed. This phase should also include site surveys of the facilities and relevant IT infrastructure.

Phase 2b: Procurement.

In this phase, the organization specifies the RFID components that must be purchased, the feature sets and protocols they must support, and any standards on which they must be based.

Phase 3: Implementation

In this phase, procured equipment is configured to meet operational and security requirements, RFID data is integrated with legacy enterprise systems, and staff are trained in the proper use and maintenance of the system.

Phase 4: Operations/Maintenance

This phase includes security-related tasks that an organization should perform on an ongoing basis once the RFID system is operational, including conducting periodic security assessments, applying security-related software patches, and reviewing RFID event logs.

Phase 5: **Disposition**

This phase encompasses tasks that occur when a system or its components have been retired, perhaps as a result of a significant upgrade. These tasks include preserving information to meet legal requirements and disabling or destroying tags and other components when they are taken out of service.

Organizations are strongly encouraged to adopt the recommended practices. Failure to implement them significantly increases the risk of an RFID security failure. Organizations should also examine each of the practices to determine their applicability to the target environment. A practice should be rejected only if it is infeasible or if the reduction in risk from its implementation does not justify its cost.

VIII. Implementation of RFID Security

Case Study: Supply Chain Management of Hazardous Materials

The Radionuclide Transportation Agency (RTA) oversees the movement of radioactive research materials between production facilities, national laboratories, military installations, and other relevant locations. The RTA oversight of the supply chain for these materials involves many of the same issues as in most any other supply chain. The agency wants to know who is in possession of what quantity of materials at any given time. It also wants to locate materials at a site quickly, without having to search through numerous containers to find them. Bar code technology does not provide that capability.

Some of RTA's requirements are more unique. For instance, much of the transported radionuclide material must be closely monitored because extreme temperatures or excessive vibration can make it useless for its intended applications. Consequently, RTA wants temperature and vibration sensors to continuously measure environmental conditions and record readings on the tag. Additionally, the handling of RTA-regulated materials is a homeland and national security issue. If the materials were to fall into unauthorized hands, they could endanger the public welfare.

Phase 1: Initiation

The project team began with a risk assessment, which identified a number of concerns, the most significant of which were as follows:

1) An adversary could identify and target a vehicle containing RTA-regulated material.
2) An adversary could eavesdrop on tag transactions to learn the characteristics of the material, which could help determine whether it is worth stealing.
3) An adversary could damage or disable a tag, making it easier to steal material without detection.
4) An adversary could alter sensor or manifest data stored on the tag in an effort to undermine the business processes for which the material is being used.
5) The radiation from readers could accidentally cause combustion of collocated volatile materials when several of them are operating concurrently in close proximity.

To help address the risks, RTA established a policy that required that tagged items only be identifiable during embarkation, debarkation, and storage, but not during transport. The policy further stated that tag-reader communication should be authenticated whenever technically feasible with commercial-off-the-shelf systems. The RTA conducted a privacy assessment that identified that the system would handle PII due to the need to associate materials with particular individuals, although most such information was already contained in existing logs. The agency updated its privacy disclosure statement for employees and contractors to account for the new technology. Finally, it required that all personnel involved in handling of the tagged materials be provided RFID security and privacy awareness training. The agency already had a HERF policy, but everyone agreed the introduction of the RFID system would require the agency to revisit the efficiency of these HERF-related controls.

Phase 2: Acquisition/Development

The acquisition/development phase focused on the planning and design of the RFID system. The nature of the supply chain was such that tagged items would be located at numerous facilities, including future facilities not yet known at time the design was created. However, some general parameters were known. For instance, readers would need to read tags from distances up to 10 meters, and this capability is typically only found in active tags.

The design team spent a significant amount of time on how to mitigate risks associated with the RF link between the readers and the tags. It determined that the risk of eavesdropping and rogue RFID transactions could be within acceptable levels if adversaries were located at least 100 meters from the storage area. The few facilities that could not maintain a perimeter of that distance would rely on bar code technology, which RTA understood would significantly increase labor costs at these sites relative to those using RFID because people would need to be hired to scan items and open containers to inventory their contents.

To address the requirement of preventing readings during transport, the design team specified mechanisms for shielding containers and vehicles. The shielding would prevent adversaries from determining that items inside a vehicle were tagged, thereby reducing the risk of targeting. In the case of shielded transport vehicles, tags could be read when they were removed from the vehicle at debarkation. Many vehicles were shielded prior to the RFID program to prevent harmful radiation from escaping the vehicle. When vehicles were not shielded, tarp-like shielding could be placed around containers within the vehicle and then easily removed when they leave the vehicle. While some users would benefit from the convenience of reading tags from outside the vehicle, the risk this introduced outweighed any potential advantage it offered. Indeed, the primary objectives of the RFID system were to identify the facility at which a radionuclide sample was located and to quickly find items once stored, neither of which necessitated readings when the item was in transport.

The tags were also password-protected using a proprietary technology to prevent unauthorized parties from reading or writing to the tags. Because custody of the tags moved from one organization to another, the RTA decided to host a central password database that could be remotely accessed by the RFID middleware of each participating organization. To limit access to the central database to business partners, it was placed on a VPN called RTAnet to which each of the partner organizations connected. The VPN isolates the RFID activity from public networks, thereby making it difficult for an outside adversary to perform a successful attack.

The team also had to tackle the HERF risk. Although the probability was small that readers would cause combustion of volatile materials stored near radionuclide material, the devastating consequences of its realization still made it a significant concern. The primary mechanism was to use an HF system because it would be less likely to cause combustion than higher frequency UHF and microwave technology. New guidelines also required a separation of five meters between fuel and tagged items unless the volatile materials were shielded.

Phase 3: Implementation

The implementation phase was straightforward, given the extensive planning in the previous phase. The first task was to conduct a pilot test of the system to identify potential problems before they adversely impacted the full supply chain. The test exercise uncovered several interoperability issues with RTAnet devices. In particular, some of the readers did not work properly with the middleware because an undocumented feature conflicted with the settings RTA selected for its equipment. The vendor issued a patch to its software that solved the problem.

Phase 4: Operations/Maintenance

Once the system was fully operational, the RTA was able to obtain regulatory information more quickly than before, which reduced the labor time required to support the program. Suppliers and consumers of the regulated materials also decreased their paperwork. They also were able to better match supply of materials with demand for them, since authorized organizations could retrieve information about the quantities present at each site.

The operations phase also included security monitoring. All participating organizations signed a MOU that covered sharing of information pertaining to possible intrusions or security exploits and proper management of PII. The MOU also included a provision that prohibited participating organizations from using PII for any purpose not explicitly stated in the MOU. This close cooperation enabled one of the suppliers and a national laboratory to recognize a recurring attack pattern across facilities that might otherwise have been ignored.

Phase 5: Disposition

As a new program, RTA has not actively confronted disposition issues. It plans to instruct participating organizations to retire their RFID systems as they would any other system holding data that RTA deems sensitive. In most cases this involves using disk wiping utilities to delete sensitive files. With regard to tag disposition, RTA's position is that organizations are free to recycle tags so long as they clear sensor and manifest data before affixing a tag to a new item.

IX. Summary Of Findings

Upon reviewing the literature and carefully analyzing the reported data supporting RFID implementation, it is clear that suppliers cannot ignore its importance in Supply Chain Management. Wal-Mart and other retail marts have stipulated conditions under which suppliers must adopt RFID infrastructure to its existing ERP systems, which of course, will require changes to their business processes which would all entail significant capital investments. Essentially, organizations would require new software, hardware and definite re-engineering of their process operations. Given the extensive capital outlay, only 20.2% opted for early adoption, 42.7% for medium adoption and 37.1% accounted for late adopters (Aberdeen Group). While the benefits to adoption were previously outlined, what appears to be certain is that RFID technology has not sufficiently progressed where results from Supply Chain Management can produce measurable. RFID systems can provide high value to the firm as it strives to achieve total supply chain visibility, unfortunately, its feasibility becomes more difficult.

X. Conclusion

RFIDs have tremendous opportunities for increasing value to a firm by providing increased product visibility, reduce out-of-stock items, trim warehouse costs, eliminate stock errors, reduce theft and shrinkage and allow companies to regularly update their logistics and inventory databases. Furthermore, it enables firms with such capability to competitive globally. Organizations such as Wal-Mart and other retail giant are spearheading RFID compliance and have set a deadline for January 1, 2005 for its top suppliers. Unfortunately, achieving this mark will present some difficulties because RFID technology has a number of operational factors which can adversely impact its efficient operation. For instance, organizations must address issues regarding RFID command language, the presence of moisture, inclement weather, radiation, invisible RF interference (i.e., WLANs), attenuation, reflection and refraction of radio waves, the material to which a tag is affixed and to some extent building material content. Additionally, RFID operating standards do not exist for global operation, which would make tracing and tracking difficult for both import and export goods. Continued research needs to be carried before RFID can realize its full implementation at a reduced cost structure.

REFERENCES

[1] B. Fabian, and O. Günther, "Security Challenges of the EPCglobal Network," *Communications of the ACM*, vol. 52, no. 7, pp. 121-125, July 2009

[2] G. Kalkbrenner, "Ubiquitous Media with UPnP and RFID-Based User Interfaces," *International Journal of Communications, Network and System Sciences*, vol. 2, issue. 2, pp. 163-168, May 2009

[3] J. Cao, L. Shu, and Z. Lu, "Synchronous Dynamic Adjusting: An Anti-Collision Algorithm for an RF-UCard System," *International Journal of Communications, Network and System Sciences*, vol. 2, issue. 2, pp. 8-20, Feb. 2009

[4] E.W.T. Ngai, A. Gunasekaran, "RFID Adoption: Issues and Challenges," *International Journal of Enterprise Information Systems*, vol. 5, issue. 1, pp. 1-9, Jan-Mar 2009

[5] M. Hayes Weier, "Coke's RFID-Based Dispensers Redefine Business Intelligence,"*InformationWeek*, June 6, 2009 [Online] Available:*http://www.informationweek.com/news/mobility/RFID/showArticle.jhtml?articleID=217701971*

[6] E. Welbourne, L. Battle, G. Cole, K. Gould, et al. "Building the Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet Computing*, vol. 13, issue. 3, pp. 48, May 2009

[7] R. Torrance, "RFIDs Power Themselves," *EDN*, May 5, 2009 [Online] Available:http://www.edn.com/article/CA6655988.html

[8] M. Anderson, "RFID Chips Gain Computing Skills," *IEEE Spectrum* (North American Ed.), vol.46, issue. 5, pp. 16, May 2009

[9] V. Matta, D. Koonce, "Semantic Breakdown of RFID Functionality to Support Application Development," *The Journal of Computer Information Systems*, vol. 49, issue. 3, pp. 54-59, Spring 2009

[10] J.K. Visich, J.T. Powers, and C.J. Roethlein, "Empirical applications of RFID in the manufacturing environment," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol.2, issue. 3/4, pp. 115-132, 2009

[11] S.A. Vowels, "RFID and the cash-to-cash cycle," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol.2, issue. 3/4, pp. 133-164, 2009

[12] S. Du, L. Xi, E. Pan, and C.R. Liu, "Design of measurement system for quality improvement in multi-stage manufacturing systems," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol.2, issue. 3/4, pp. 165-182, 2009

[13] W.L. Wang, S.J. Wang, and A. Chen, "The impact of introducing RFID patrol system into rolling mill manufacturing: an empirical study on maintenance management," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol.2, issue. 3/4, pp. 183-194, 2009

[14] S.J. Wang, W.L. Wang, and S.F.Liu, "The configuration of a multi-agent-based inventory replenishment simulation system for RFID-enabled TFT-LCD supply chain," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol.2, issue. 3/4, pp. 195-215, 2009

[15] Y. Luo, Y.T. Lee, "Data exchange strategy for manufacturing simulation of shop floor information systems," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol.2, issue. 3/4, pp. 216-227, 2009

[16] E. Bottani, "On the Impact of RFID and EPC Network on Traceability Management: A Mathematical Model," *International Journal of RF Technologies: Research and Applications*, vol. 1, issue. 2, pp. 95–113, 2009

[17] B. Todd, M. Phillips, S.M. Schultz, A.R. Hawkins, and B.D. Jensen, "Low-Cost RFID Threshold Shock Sensors", *IEEE Sensors Journal*, vol. 9, issue. 4, pp. 464-469, Apr 2009

[18] F. Thiesse, C. Floerkemeier, M. Harrison, F, Michahelles, and C. Roduner, "Technology, Standards, and Real-World Deployments of the EPC Network," *IEEE Internet Computing*, vol. 13, issue. 2, p. 36, Mar. 2009

[19] S.S. Saab, W. Mhanna, and S.Saliba, "Conceptualisation Study for Using RFID as a Stand-alone Vehicle Positioning System," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol. 2, issue. 1/2, pp. 27-45, 2009

[20] D.D. Arumugam, A. Gautham, G. Narayanaswamy, N. Ayer, and D.W. Engels, "Impact of Human Presence on the Read Zones of Passive UHF RFID Systems," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol. 2, issue. 1/2, pp. 46-64, 2009

[21] C.P. Hohberger, and B.Y. Tsirline, "Design of a 13.56 MHz Segmented Helmholtz Coil for RF Exposure Testing of Biologics to Simulated RFID Readers," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol. 2, issue. 1/2, pp. 65-92, 2009

[22] J.D. Porter, T.A. Bruno, and J.M. McKee, "Performance Characterisation of Semi-active RFID Technology," *Intl. Journal of Radio Frequency Identification Technology and Applications*, vol. 2, issue. 1/2, pp. 93-114, 2009

[23] M. Jo, H.Y. Youn, S.H. Cha, and H. Choo, "Mobile RFID Tag Detection Influence Factors and Prediction of Tag Detectability", *IEEE Sensors Journal*, vol. 9, issue. 2, pp. 112-119, Feb 2009

[24] S. Gaudin, "Food Poisoning Outbreaks Could Prove a Boon to RFID," *ComputerWorld*, vol. 43, issue. 4, pp. 10-11, Jan. 25, 2009

[25] J.G. Fernandez, J.C.Y. Garcia, Y.-S.M. Garcia, and J. Santos, "Transf-ID: Automatic ID and Data Capture for Rail Freight Asset Management", *IEEE Internet Computing*, vol. 13, issue. 1, pp. 22-30, Jan 2009