

1. Radio Frequency Identification (RFID) primer

TODO

1.1. History of RFID and current expectations of the technology

Much of the literature about RFID focuses on the accelerated activity performed in the last five years since the formation of EPCGlobal™. However, radio frequency identification has been used since World War II to solve identification and asset tracking problems. Progressing through its history with a focus on specific aspects of the individual usage scenarios gives an insight into how current expectations have formed.

The first known use of Radio Frequency Identification was during World War II. The British Royal Air Force used the technology as an identification tool in its Identify Friend/Foe (IFF) systems. Allied planes outfitted with an IFF transponder would respond to queries from ground-based radars with a specific response; Axis planes could then be identified since they would not respond to the signal [i].

All remote IFF transponders would respond with the same signal, and so IFF was not used to identify individual planes. The later use of RFID for preventing inventory shrinkage is a similar usage scenario, since the presence or absence of a signal is sufficient data to require a reaction. The fact that the system was not line-of-sight and could operate under adverse weather conditions was fundamental to its usability. This continues to be a stated advantage of RFID.

A number of research laboratories and private firms continued to improve the technology, specifically on adding the capability for unique identification of individual transponders [ii]. By the late 1970s, RFID was being used for the tracking of livestock. Individual heads of cattle were tagged with their own identification beacon, usually implanted under the skin or on the ear. RF readers were placed at points of entry into barns, feeding stalls and other locations.

The ability to identify individual cows without human interaction allowed better tracking of feeding and health irregularities. Unique identification has since become a feature of current RFID usage scenarios. The RF tag also replaced the older process of branding cows with a hot iron. This had advantages in terms of employee safety. This is often identified as a possible advantage of RFID when compared with repetitive stress disorders caused from manual scanning of barcodes. Up to a third of a cow's leather output can be ruined during branding, and here RFID also offered industry-specific advantages []. Companies have continued to find significant advantages in using RFID beyond the more commonly documented expectations. Even though these do not translate into other industries, they are nonetheless important.

By the early 1980s, railroad companies were using RFID to tag rolling stock. This was among the first uses of RFID for asset tracking over a large geographic area. An earlier initiative with bar codes failed due to poor read reliability in adverse weather conditions, high travel speeds and especially direct sunlight [1]. While read reliability of passive RFID tags continues to lag expectations, many users are planning for a possible future in which they are good long-term tracking solutions compared to competing automatic identification technologies.

By the early 1990s, RFID had arrived in suburban malls throughout the United States as an enabling technology for Electronic Article Surveillance (EAS). RFID readers positioned by store exits would trigger an alarm if an EAS tag passed through the field.

The capability of the tags was limited to the same level of functionality as the IFF transponders of five decades ago, and only indicated the presence of the tag in the field. It was the first major use of RFID for controlling inventory shrinkage, a usage scenario which is driving many companies to invest in RFID. In addition, these tags were relatively low-cost and did not require a battery for power. While the read range was limited, this was one of the first widespread uses of passive RFID tags. The majority of this thesis focuses on this type of tag.

Around the same time, RFID was being used to identify vehicles during the collection of road tolls. A vehicle would have a battery powered transponder attached to the windshield, which would be read as the vehicle passed through a toll portal at highway entrances and exits.

The term “RFID license plate” probably comes from this early use of the technology, since only a unique identifier is read from the transponder. This identifier is then cross-referenced with a separate database containing billing information. While this is not the first significant IT implementation supporting an RFID-enabled automatic identification system, it was one of the first that the public became aware of. In Dallas, a TollTag® could be used to pay tolls on the North Dallas Tollway, pay parking at the airport and at downtown parking garages and also gain access to third party business campuses [2]. The requisite sharing of IT data presaged similar requirements in current supply chain visibility applications.

The United States Department of Defense (DoD) was becoming involved in RFID during the 1990s due to the identification of supply chain challenges. During Operation Desert Storm in 1991, logistics and materiel distribution was a major problem. The Defense Logistics Agency (DLA) became known for “iron mountains” of unopened shipping containers in the middle of the Saudi Arabian desert [iii]. The lack of supply chain visibility required 25,000 of the 40,000 containers to be opened in order to identify their contents [iv]. A Defense Research Projects Agency (DARPA) grant was awarded to Savi Technology to identify whether RFID could help prevent similar supply chain problems in the future. This resulted in several initiatives over the next few years.

Evaluations of the Defense Logistics Agency's effectiveness during Operation Desert Storm focused on the high cost of the DLA's supply chain. In 1995, the Joint Total Asset Visibility office was formed with a charter to provide asset visibility in-storage, in-process, and in-transit to optimize the DoD's operational capability [v]. This had several results. First, it organized all RFID supply chain initiatives under one office, instead of being managed by individual armed forces or distribution depots. Second, it provided a source for funding future RFID initiatives. By 2004, the DLA had spent over \$100 million on RFID initiatives; this level of funding would not have been available under the previous organizational structure [vi]. Finally, the implementation plan tied RFID usage to the overall strategic goals mandated by the department's charter. This forced a necessary pragmatism around RFID's relative advantages compared to other automatic identification technologies. These realistic expectations were a key contributor to the success of the DLA's RFID initiatives.

By 2004, the DoD had joined EPCGlobal™, an organization described later in this chapter. In 2004, it ran a pilot implementation using active and passive RFID tags attached to Meals-Ready-To-Eat (MRE) combat rations under the Combat Feeding Program [vii]. The rations were tracked from the vendor to the consuming unit through several supply chain participants and locations.

The pilot was important for several reasons. The DoD was using passive RFID tags on a difficult-to-read material: MREs are packaged in metal foil. The active tags involved also tracked temperature variation in order to better determine the final shelf-life of the MREs. The combination of sensors and RFID provides the DoD with significant capabilities in tracking supply chain quality in several key classes of material, especially ordnance and perishables.

Finally, the value of end-to-end supply chain visibility with RFID cemented the importance of having DoD suppliers participate in RFID implementations. The DoD RFID Policy was finalized several months later, and is described in section 1.5.5.

1.2. Tag and reader communication

A layman's understanding of how tags and readers communicate is helpful in understanding the complications that arise when evaluating, architecting and implementing RFID systems.

In many ways, the physical processes involved are the same across all types of wireless communications systems, including WiFi, cordless telephones, and even baby monitors. There is a transmission of an interrogator signal from an antenna to a transponder, and a separate transmission of a reply from the transponder to a receiving antenna [viii]. Most interrogator designs allow for a single antenna to be used for transmission and reception.

The RFID hardware components referenced in this thesis achieve far-field coupling through the transmission, propagation, and reception of electromagnetic waves [ix]. The RFID tags referenced in the DoD's policy document work at a frequency

around 900 Mhz. At this frequency, energy propagation under far-field dynamics predominates at ranges greater than 50mm [].

In the presence of an electromagnetic field, an RFID tag's antenna functions as a voltage generator. This current powers a microprocessor which modulates the radar cross-section of the tag and therefore its reflected power. The modulation applied is usually specific to the tag, and so information on that tag can be sent to the receiver [x].

The information transmitted is usually a binary string. Depending upon the usage, the length of this string can be anywhere from a single bit to many kilobytes of data. The necessary length is driven by the needs of the usage scenario and constrained by cost and the capability of current technology. The tags referenced in the majority of this work store between 64 or 96 bits of usable data. The format of the information is described in section 1.5.3.1.

The ability of a transmission field to successfully power a tag and a receiver to collect the reflected signal is affected by a variety of factors. This, in turn, affects the reliability of tag reads within a field. Most of these factors are characterized in Figure 1.

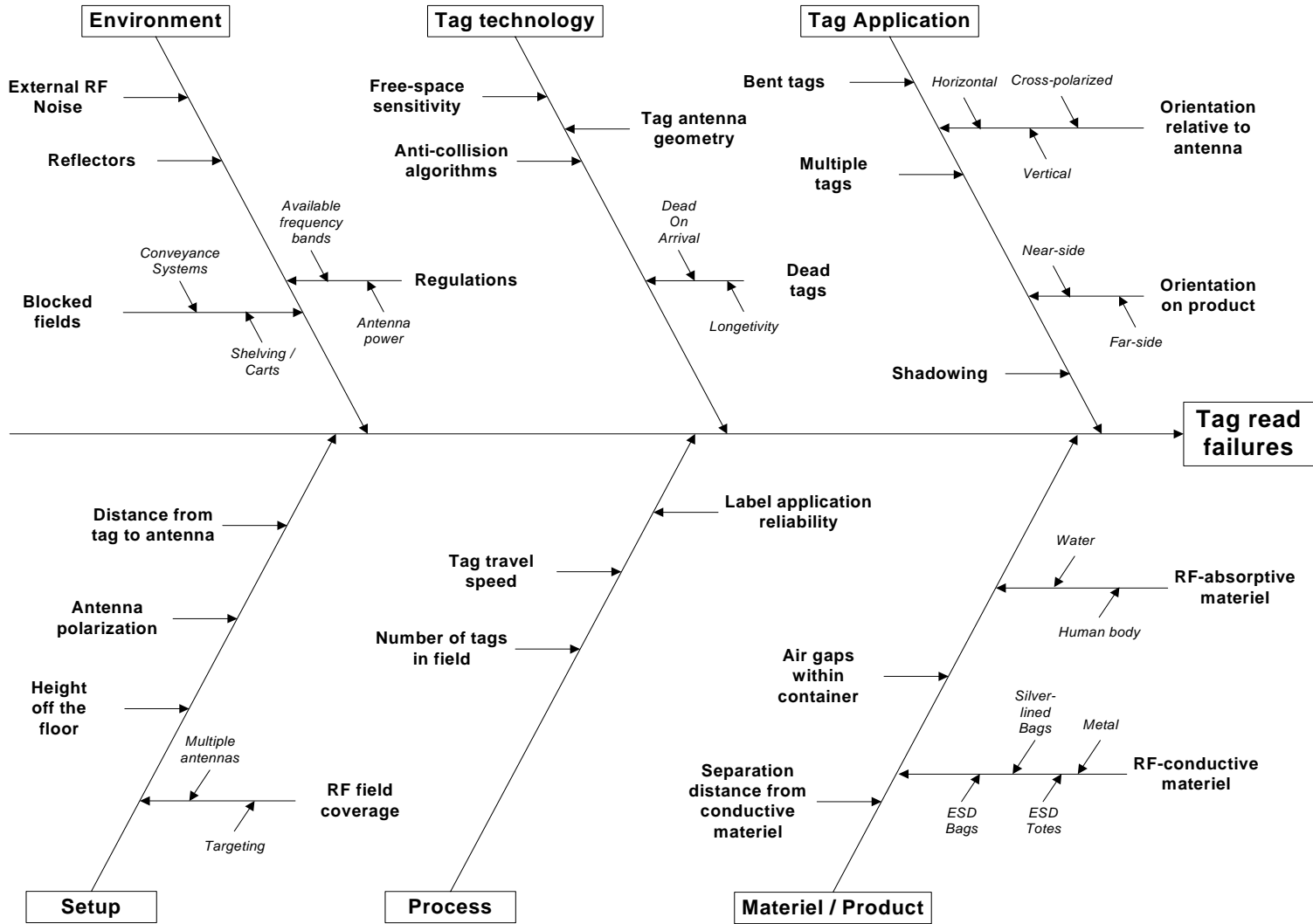


Figure 1: Fishbone analysis of tag read failures

This work does not delve into the specifics of how physics and electromagnetic field theory affect an RFID implementation. Nonetheless, RFID is a technology based on physical phenomena and governed by their immutable laws.

1.3. Benefits of RFID as an automatic identification technology

Several automatic identification technologies already exist. Barcodes were first implemented in the 1970s, and became ubiquitous in the following decade. [TODO: other technology from DoD presentation]. The DoD has had success with memory contact buttons, which can store large amounts of information. Each of these technologies has to compete with old-fashioned manual marking and identification; in many cases the old-fashioned method is still the most appropriate.

RFID offers a suite of capabilities, which when taken together make it better suited for a variety of usage scenarios.

1.3.1. Field-based area identification

Unlike most other automatic identification technologies, RFID does not require line-of-sight in order to read or write marking information. The electromagnetic field radiated from an antenna is usually a wide cone, and several multiplexed antennas can effectively cover a dock door or similar portal. Any tag entering this field can be identified. In comparison, a barcode must be presented to a reader, while memory buttons require physical contact.

This feature of RFID provides many advantages. Pallets and containers do not need to be broken down in order to identify their individual components. The orientation of packages is less important, and the human interaction with high-volume automated processes can be simplified. In some cases, RFID can be used where the physical environment precludes the use of barcodes: barcodes on railcars did not work in inclement weather.

There are some disadvantages, however. It is far more difficult to identify individual tagged material with RFID. The Raytheon training class begins with an exercise to separate similar tags from a large disorganized set of tags. It usually takes participants some time to realize that they must physically separate the tags in order to read just one at a time. This problem can be removed with the addition of human-readable information or a modification in the business process.

1.3.2. Fast reads and high throughput

RFID also allows tag reads at extremely high speeds. Current interrogator models can read a single tag several hundred times a second, and multiple tags at over fifty times per second. In real-world environments it is difficult to achieve reliable reads of all the tags in the field, but this is likely to improve as the technology matures.

There are several implications of this capability. There is little improvement over other technologies in scenarios where a single tagged product is being read at a time. Companies have been successful at reading tags on a conveyor moving at 600 feet per second. However, this is more a requirement of the existing conveyance infrastructure than an enabling technology.

The ability to read multiple tags at high speeds is the key capability. The usage scenario described in section 1.3.1 Field-based area identification is more effective if the forklift does not need to stop while the cases are being identified. The cycle time reductions which result from this capability contribute towards the benefit calculations in most return on investment analyses.

1.3.3. Memory storage and unique identification

The third capability driver is the ability of RFID tags to hold a large amount of information. A simple barcode usually stores between 20 and 30 bits of data. This is more than enough to uniquely identify a manufacturer and a product type. One is unable, however, to distinguish between two items of the same product. For example, two identical boxes of cereal will have the same UPC code.

Passive RFID tags can store 96 bits of data, more than enough to uniquely identify every atom in the universe. A more practical use is the ability to uniquely identify individual items being manufactured. This allows the tracking of individual items through the supply chain, and makes usage scenarios based on shrinkage reduction and counterfeit protection feasible.

Active RFID tags can store even more information. Currently available products offer up to 256 kilobytes of storage space, but larger amounts are certainly possible. This amount of memory is often used to store manifest data on the products within a container. Active RFID tags are sometimes connected to sensors, and the onboard memory is used to store a profile of temperature, vibration or other environmental characteristics.

1.4. Components of a complete RFID system

Over the past few decades a certain dominant design has emerged for complete RFID systems. In general, a system is composed of hardware, software and business processes. More recent events in the vendor landscape have suggested the possibility that some of these components are converging. For example, hardware components now contain some of the functionality previously provided by standalone software.

1.4.1. Hardware

The hardware components of an RFID system are usually very easy to identify. At a minimum, this includes:

- **Tags, which are programmed with binary data and respond to commands propagated through the electromagnetic field;**
- **Fixtures which attach the tag to the object being tracked;**
- **Interrogators (often called readers), which power antennas to transmit commands to tags and interpret the modulated results;**
- **Antennas which transmit and/or receive data by propagating the electromagnetic field;**
- **Network infrastructure, to allow communication between interrogators and the enterprise systems which evaluate hardware data;**

- **Power infrastructure, to provide power to the readers. Most current readers require AC power, while handheld models use rechargeable batteries.**

There is often significant product variety in each of these component categories. Tags can be classified into two main types: passive and active. Active tags have an onboard battery which amplifies the transmitted signal and/or powers the semiconductor chip. At frequencies around 900Mhz, these can be read more than 30 meters from an antenna. Active tags are relatively expensive, but can often store large amounts of information and are appropriate for some usage scenarios.

Passive tags do not have an onboard power supply, and their semiconductor chips draw power from the electromagnetic field it is in. This reduces both the useable range and cost by an order of magnitude. The antennas on passive tags are often tuned for specific orientations or fixturing scenarios, and a wide variety of tags are available. Passive tags hold only 64 or 96 bits of user-programmable data, much less than what is available on active tags. This is enough, however, to uniquely identify and serialize a manufacturer's products in the supply chain.

Most passive RFID tags are sold in one of two fixturing modes. Some are available as small adhesive inlays which can be peeled off and stuck onto a product or packaging material. Others are embedded into standard sized label rolls. These work are fed into an RFID label printer which prints barcodes and human-readable data while programming the tag. These "smart labels" are then affixed to the product or packaging material.

Interrogators come in a wide range of capabilities and formats. The majority are "black boxes" with connectors for antennas, power and networking. Others are embedded into label printers as described above or handheld units similar to barcode scan guns. The functionality they can support also varies. Many provide some filtering capabilities in order to identify events and export data in compliance with industry standards. At the other end of the complexity spectrum, some interrogators simply sound a siren if a tag enters the field.

Antennas are far simpler. These are usually very simple hardware components, containing metal strips or plates in a rugged housing. Coaxial cable connects the antennas to the interrogator. The interrogator modulates the power to the antennas, creating the electromagnetic field. Some interrogators multiplex several antennas in order to cover a larger area with a single virtual field.

The network and power infrastructure is an oft-forgotten aspect of every RFID system. Interrogators have input/output capability in the form of RS-232 (serial) ports, Ethernet ports, 802.11b wireless cards, or proprietary RF protocols. Obviously this requires something to connect to. Power infrastructure usually means AC power, since the antennas are powered at up to 4 watts [TODO reference to Scharfeld?]. Power limitations generally limit portable readers to line-of-sight applications and short bursts of activity.

For reference purposes, the table below shows the cost of many of these components in 2004. These are not average or median values, but representative of a rough order of magnitude. Significant price reductions are possible when hardware is bought in large quantities.

Hardware subcomponent	Cost in US Dollars
Active tag (minimum price)	\$1.50
Passive tag	\$0.30
EPCGlobal™-compliant fixed interrogator	\$2,000.00
Antenna	\$200.00

Table 1: Representative costs of hardware components in 2004

1.4.2. Software / Middleware

RFID interrogators can provide a great deal of data or very little useful information in the absence of software (depending upon your viewpoint). The interrogator can identify that one or more tags are in the presence of a field irradiated by its antennas, and do this many times a second. This is not very useful in and of itself, since most usage scenarios require information on changes that occur. The fact that a new tag has been identified within the field could mean one thing; the sudden absence of a previously identified tag would indicate something different. Reading the same tag from the same reader over and over again, however, means very little.

The information of value to supply chain applications are the events corresponding to movement of tagged material between multiple interrogators. Software, termed “middleware”, interprets events from the raw data streaming from an array of interrogators. More importantly, it coordinates the updating of information in other enterprise systems like MRP, ERP and CRM.

For example, middleware may recognize that a specific tag has disappeared from the field of one interrogator only to appear in the field of another. If the first interrogator is situated at the outbound dock door of a manufacturing plant and the second is situated at the inbound dock door of a distribution center, this probably indicates that a finished product sent from the plant has arrived at the distribution center. In this event, middleware might credit and debit the appropriate accounts in an enterprise cost accounting system, update the order status in a customer’s extranet portal, and place a replenishment order in the manufacturing plant’s MRP system.

Interfacing with enterprise IT systems can be a time-consuming and expensive project. The vast amount of data produced by the RFID infrastructure and the need for redundancy due to performance limitations complicate this further. In one early manufacturing implementation done by a consulting firm, \$1,425,000 of the initial \$1,710,000 investment was attributed to business process, application and system integration costs [11].

1.4.3. Business processes

Feature-rich middleware solutions often provide the ability to overlap supply chain process diagrams onto a physical network of RFID interrogators. This lets the software translate interrogator event signals into knowledge about the movement of material through the supply chain. However, this interpretation can

often be very difficult since material in real-world supply chains does not always follow the same physical flow.

There are several possible causes for this. Human material handlers may not be disciplined about material placement within a facility, resulting in tags passing through the wrong interrogator fields. Tags may be inadvertently blocked or permanently disabled on accident, resulting in a loss of visibility information. Finally, the documented process may be substantially different from real-world behavior. This behavior often evolves into a complex fire-fighting system erected to bridge the gap between IT systems, customer requirements and the documented process.

Most substantial RFID implementations will require large changes to the current business processes in order to take full advantage of the technology's capabilities. Overlaying an RFID infrastructure onto existing business processes is likely to solidify inherently inefficient methods. This has been likened to "paving the cowpaths" which existed in Boston's North End: less effective than rethinking the transportation network in light of technological advances [12].

The effort required to develop and implement these changes to business processes can be substantial. Wholesale modification to existing systems is complicated by the limitations of current technology. Redundant systems, like barcodes and manual entry, will need to co-exist with RFID until the technology is sufficiently reliable. The warehouses of many companies have not seen significant change since the rollout of warehouse management systems, and a new technology will be entering an environment slow to adopt change.

Still, the majority of RFID investments will only achieve high returns in conjunction with business process improvement. This often ignored third component of a complete RFID system is as fundamental to its success as either hardware or software.

1.5. Industry structure and the role of EPCGlobal™

As enterprises became interested in using RFID to improve the performance of their supply chains, an overall value chain structure became apparent in the RFID system industry. It was in everyone's interest to ensure that RFID did not stumble on the same obstacles that slowed adoption of previous technologies like the barcode. A consortium named EPCGlobal™ was formed as a result of this evaluation. This section describes the players in the RFID value chain, some challenges this industry structure poses, and how EPCGlobal™ attempts to meet these challenges.

1.5.1. Value Chain Analysis

Figure TODO shows an abstracted view of the value chain for RFID systems. This includes the components described in 1.4 Components of a complete RFID system and the information which results from tracking RFID tags through to the end consumer. A description of each segment of this value chain provides a foundation for understanding the challenges facing the adoption of RFID.

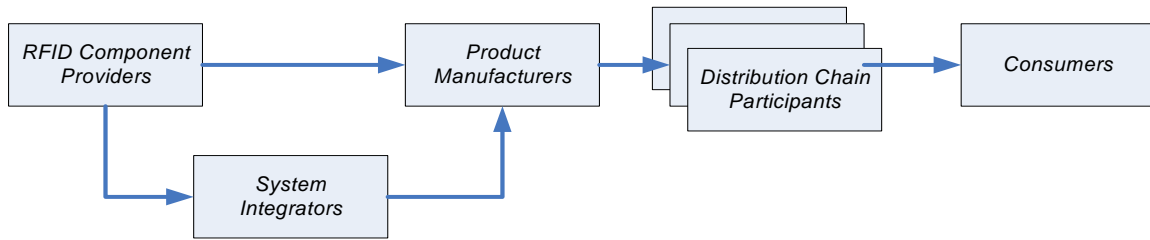


Figure 2: RFID Industry Value Chain

At the source of the chain are RFID Component Providers. These hardware and middleware companies make hardware and software components for the completed systems. These providers sometimes work directly with Product Manufacturers who have chosen to in-source their implementation projects. Of those RFID Component Providers that already have products in the market, the majority are small startups focused exclusively on developing components for complete RFID systems. Larger, established companies are only beginning to provide middleware solutions, and few have entered the hardware space. However, it is expected that consolidation and acquisitions will occur, and this part of the value chain will see a lot of changes in the future.

System Integrators work with RFID Component Providers to provide the business process components and integration required for a fully functional RFID system. System Integrators' experience helps Product Manufacturers shorten the learning curve and overcome the difficulties of working with early stage technologies. The large consulting companies have made a significant investment in helping their clients implement RFID. Several smaller system integrators also exist in the marketplace, but any consolidation that occurs will happen for reasons other than RFID.

Product Manufacturers purchase RFID components either separately or as a complete system. Raytheon Integrated Defense Systems falls into this category of value chain participants. A Product Manufacturer's core business is making products for end consumers, and RFID is simply an enabling supply chain technology. In most cases, these are the companies applying tags to individual cases or pallets of material and enter the corresponding "traveler" information into product tracking software. The level of investment in RFID is dependent upon the approach taken by the manufacturer. Some will simply "slap and ship" a tag onto product as it leaves the dock.

Distribution Chain Participants are the departments within Product Manufacturers and / or third-party companies which deliver the product to the end consumer. They are participants who did not apply the tag to the material but have the opportunity use the tag information to track the product as it flows through the distribution channel. They will often have purchased RFID system components themselves, but mostly to read the tags of Product Manufacturers. These companies may be able to reap significant benefits through the additional supply chain visibility RFID provides.

The value chain usually ends with the final consumer of the tagged product. These consumers could be a Wal*Mart® shopper in Texas or an U.S. Army infantry

soldier in Iraq. Some will be concerned by factors like price and product availability, while others will also want to be assured of freshness and product safety. RFID may provide the ability to reduce cost and improve services levels for these consumers. Some consumers will be concerned by the privacy ramifications of RFID, while others will not.

In some instances, there will be a reverse logistics value chain in which the product is returned to upstream participants for service or disposal. This does not significantly affect the analysis of the industry, however, as the issues involved are similar.

1.5.2. Challenges posed by the RFID value chain

This industry structure poses several challenges to the adoption of RFID. One obstacle is the relationship between the Product Manufacturers and the Distribution Chain Participants. While some companies work directly with the end consumers, in the majority of product categories there are multiple organizations involved in getting the product to the consumer. This leads to several challenges.

1.5.2.1. Challenges in coordination of the supply chain

First is the large amount of information communication which needs to occur between the distribution chain participants. A single participant, like Wal*Mart®, sources products from a large number of companies, but cannot manage an infinite number of RFID data formats and sources. Some information transport standards will be necessary in order for this to work. In addition, products must be uniquely identified across all the suppliers, as they are with barcodes.

If the consumers are concerned about the route or environment their product has traveled, this information transport is even more important. This consumer need has been voiced in the pharmaceutical industry, where counterfeit drugs present a safety problem. It is also important in industries like defense, where vibration, humidity or temperature extremes can negatively affect the performance of ammunition and other equipment.

The Product Manufacturer and Distribution Chain Participants may be located in different countries, and this presents another challenge. Different countries have different laws which govern the use of ultra-high frequency communication, and so RFID hardware and business processes may not be consistent across the entire distribution chain.

In many cases, the costs of implementing RFID are borne by the Product Manufacturer, while benefits largely accrue to those in the distribution chain. Ongoing costs are the purchase and application of tags, while benefits will be based on gains achieved by using the data contained within the tags. This coordination problem can be exacerbated by differences in organizational power within the value chain. Effective communication and a method for transfer pricing might help alleviate this situation.

1.5.2.2. Challenges with an emerging technology

Many of the advances in RFID technology are being developed at small startup companies. This is normal with early-stage technologies, but there are some drawbacks. Downstream participants are generally large established companies,

and do not expect their technology suppliers to go out of business at the rate startups generally do. The Product Manufacturers will require some assurance that their investment in RFID will survive even if one of their suppliers does not.

If it is assumed that all participants in this value chain are interested in quickly achieving widespread adoption, some other conclusions can be drawn. Product Manufacturers will help RFID Component Providers grow at rates higher than would be otherwise expected in order to speed development of the technology. However, the downstream participants will not want to be at the mercy of their RFID Component Providers once the market matures. Some peaceable solution that maintains an agreeable balance of power will be necessary.

1.5.2.3. Consumer concerns

History is littered with technological innovations that failed because they did not effectively manage the concerns of consumers. In a study of emerging technologies which failed in the face of consumer concern, technologies which did not benefit from a coordinated public relations effort had significant problems with adoption. The ability to opt-out had positive results as well [13].

Several consumer privacy groups have raised concerns about the implications of widespread RFID use, and several governments have considered legislation limiting the use of tags in a retail environment [14]. Articles overstating the capabilities of RFID have been written which imagine a privacy-free world [15]. No single company is driving RFID adoption and can take the responsibility of communicating with consumers about RFID. This could lead to significant problems in the future.

1.5.3. The role of EPCGlobal™

RFID industry participants recognized these challenges and worked with MIT and other universities to create the Auto-ID Center in the late 1990s. Founding members included several hardware and software component manufacturers, system integrators and a number of product manufacturers and distribution chain participants. Its overall goal was to drive the adoption of RFID, and the center took several steps to work towards this objective. In 2003, the administrative function of the center was spun off into an organization called EPCGlobal™, while the university research components continued under the auspices of the Auto-ID Labs [16].

EPCGlobal™ works towards its goal of driving RFID adoption in several ways. Each targets one or more of the challenges presented by the industry structure or specifics of the technology. Its success in the past several years is based on a respect for these challenges and an understanding of the history of other supply chain technologies.

1.5.3.1. EPCGlobal™ and standards

First and foremost, EPCGlobal™ establishes and promotes standards for the automatic identification of items in the supply chain of any company, industry and country [17]. In practice it has been assumed that these items would be identified through the use of RFID tags. In general, these standards can be subdivided into three main groups: the EPC number, software and hardware.

EPC is an acronym for “Electronic Product Code”. The EPC number is a compact numerical naming convention to uniquely identify items in the supply chain [18]. When an EPC-compliant tag responds to an interrogator, it usually transmits its EPC number. Current versions of the EPC contain either 64 or 96 bits, and store four pieces of information:

1. A Header that identifies the format and version of this EPC,
2. A Manager Number which uniquely identifies the company associated with the product being tagged,
3. An Object Class, which is essentially a Stock Keeping Unit (SKU) identifying a product type unique to that company, and
4. A Serial Number which uniquely identifies the item being tagged and differentiates it from other instances of the same Object Class.

The software standards serve to meet the supply chain coordination challenges described in section 1.5.2.1. The Physical Markup Language (PML) offers a common vocabulary for communicating information about items across the entire supply chain [19]. This solves the hypothetical problem Wal*Mart ® would have faced in interfacing with a large number of different data formats. PML is extensible, meaning that additional attributes can be appended as needed. Pharmaceutical companies could communicate manufacturing location data through the supply chain, while the DoD could track environmental characteristics.

Object Naming Service (ONS) provides for the translation of tag license plate data into useable information about the manufacturer and product [20]. It works in a method similar to the Internet’s Domain Name Service (DNS) which translates a human-readable address like www.google.com into an IP address like 64.233.161.104 which can be used to route information.

The EPCGlobal™ Network shares another similarity to the Internet in that manufacturer’s products, like web servers, must be uniquely identifiable. EPC numbers cannot be duplicated between manufacturers; otherwise the tracking capabilities would not work in any supply chain in which those manufacturers’ products intersect. In order to prevent this from occurring, EPCGlobal™ members are given unique manager numbers which define a namespace inside which all of their EPC numbers must exist. EPCGlobal™ maintains a close relationship with UCC and EAN, organizations which administer the barcode namespace, in order to allocate manager numbers.

EPCGlobal™ also establishes standards for some of the hardware components in an RFID system. The consortium has defined a hierarchy of tag types, labeled Class 0 through 5. Class 0 and 1 tags are the focus of this thesis, and the specifications describe read-only and read/write passive tags which can be produced at low cost. The storage capacity, features and expected cost of the other tags increase with their designation number; Class 5 tags offer much of the same capabilities as the current generation of interrogators.

While EPCGlobal™ has not outlined specific requirements for interrogators, much of their current capability is driven by the interfaces defined in the tag

specification. Antennas have not been addressed, although transmission parameters and limits are set in the US by the Federal Communications Commission (FCC) and in other countries by similar entities. There are also other standards which EPCGlobal™ has defined that we will not be discussing.

One result of these hardware standards is that they reduce Product Manufacturers' and Distribution Chain Participants' dependence upon any single RFID Component Provider. The untimely demise of one startup would not imperil the initiatives of the overall value chain. The standards also serve to limit the power of these RFID Component Providers by removing most possibilities for proprietary solutions. The standards have in effect become a suitable answer to the challenges of working with an emerging technology described in section 1.5.2.2.

1.5.3.2. A single industry voice for RFID

There are already many companies working with RFID technologies and more are being added to this list every day. An important role of the EPCGlobal™ consortium is to provide a single voice for the industry. While there are challenges in gaining agreement from all the individual members within the consortium, managing conflicts internally grants the possibility of coherent and consistent external communication. When used appropriately, the full weight of some of the world's largest companies can provide solutions to problems that would otherwise be ignored and limit adoption.

One area in which this is important is in addressing wireless spectrum regulations across the world. Countries have different limitations on the amount of power that can be transmitted from an antenna, making communications performance and reliability in global supply chains difficult to predict. In addition, frequency ranges allowed for RFID communication can differ between countries. Antenna length and other parameters are tuned for specific frequencies, and this difference can adversely affect performance. EPCGlobal™ can provide a source of power in transforming these regulations, but it is unclear whether this will occur.

The consortium provides a forum for all the value chain actors to interact, and this can lead to additional advantages. Recently a member of the consortium requested large royalties for the intellectual property it had contributed to the next generation tag specification. While the request was made in compliance with EPCGlobal™'s intellectual property policy, furor over this request may result in the standard remaining royalty-free [21]. Without a formal forum in which to have these discussions, it is unlikely that royalty-free standards would be developed.

Finally, the consortium allows a single voice in responding to consumer concern regarding privacy in an RFID-enabled world. EPCGlobal™ has issued guidelines for use by all companies engaged in large-scale deployment of EPC [22]. These dictate that customers have the right to be notified if EPC is present in a product or its packaging, and how to disable the RFID. In general, the RFID tag will be on the product packaging, and so simply discarding the packaging is sufficient. The guidelines also address a methods for informing the public on EPC and require consortium members to publish privacy policies regarding how information collected is used.

While the guidelines are commendable, it is not clear that EPCGlobal™ has succeeded in allaying the fears of the public and especially watchdog groups like CASPIAN and Electronic Privacy Information Center [23]. There is a need for a consistent and vocal public relations program if RFID adoption is to extend to the public consumer.

1.5.3.3. EPCGlobal™ and knowledge sharing

The final method in which EPCGlobal™ helps to meet the challenges posed by quick adoption of RFID is by providing a forum for sharing knowledge. A company seeking to integrate RFID into its supply chain must consider issues spanning manufacturing operations, information technology, finance, packaging design, facilities layout, and other topics. The formal knowledgebase made available to consortium members can help organizations up this steep learning curve. Frequent conferences are held, and action groups have formed in some industries to address with their specific concerns [24].

In addition, EPCGlobal™ maintains a relationship with the Auto-ID Labs at several universities worldwide [25]. The labs conduct research into various aspects of RFID systems, and continue to publish research. Through this relationship, EPCGlobal™ can help shape the direction of research in order to address obstacles adoption might face in the future.

1.5.4. The need for mandates

A challenge EPCGlobal™ does not specifically address is the lack of overlap between those who pay for RFID and those who accrue the benefits of this information. Only in some cases is the return on investment so spectacular to the manufacturer that it is feasible to implement RFID within its own organizational boundaries. On the other hand, retailers can see significant benefit if shipments arrive with RFID tags on them [26].

One example of this is Gillette's proposed use of RFID to counter shrinkage. Shrinkage is usually a euphemism for theft and loss, and occurs throughout Gillette's distribution chain. Gillette's razors are small, high-value items and easily resold once stolen. The company is currently researching methods of implementing RFID in order to reduce this shrinkage. However, this example of generating internal ROI is the exception, and usually limited to industries with high-value products [].

The question is how does an industry drive RFID adoption? One option is to develop contracts stipulating the sharing of costs and benefits across multiple parties. This type of solution is used in a number of situations where organizations are seeking to achieve a global optimum in their supply chains. However, this would be difficult to do with RFID. There are a large number of suppliers and the number of contracts required would be prohibitive. In addition, RFID is still an emerging technology. There are many unknowns in any cost / benefit calculation, and organizations may find it difficult to come to an agreement.

A more likely option is for particularly powerful market participants to mandate that other members begin an investment in RFID. This is what is happening in the retail industry. Wal*Mart and other large global retailers, will be requiring their

suppliers to tag shipments with RFID and transmit this information to them. The retailer's market power allows them to issue such a policy with a high likelihood of compliance. This has driven adoption throughout the value chain.

1.5.5. The DoD RFID Policy

Seeing a similar situation, the DoD finalized an RFID policy to its 43,000 suppliers on July 30, 2004 [27]. The information in this section is sourced from this policy statement, and citations are only used for specific figures or quotes from the statement. In broad strokes it requires defense suppliers to tag their their shipments with RFID tags. This will allows the shipments to be tracked as they travel through the Defense Logistics Agency's supply chain. This section describes the policy in detail. Although there are aspects which are specific to the defense industry, the policy is similar to those issued by companies in retail and other industries.

While the specific business rules were issued on July 30, 2004, the general expectations were publicly outlined as early as October 2, 2003 [28]. The first part of the policy describes requirements for the tagging of oceangoing containers and international shipments with Active RFID tags. This is an extension of the network the DoD has deployed worldwide and was described in section 1.1. We will focus on the portion of the policy that considers passive RFID tags.

1.5.5.1. Three dimensions of the policy rollout

The cope of the policy expands over the next few years in three dimensions:

- The types of products which must be tagged,
- The shipment's point of entry into the DoD's brick & mortar distribution network, and
- The level at which shipments are tagged: individual items, cases or pallets.

On January 1 of 2005, 2006 and 2007, the next level of the requirement is mandated until nearly all incoming containers are tagged with RFID.

The DoD organizes the products it buys into ten different classifications as shown in Table 2.

Class	Material covered
I	Meals-Ready-To-Eat (MREs), Food, sustenance, and commercially bottled water
II	Clothing, individual equipment, tools, toolkits, administrative and housekeeping supplies
III	Petroleum, oil & lubricants, bulk fuels
IV	Construction items
V	Ammunition and ordnance
VI	Personal demand items, health & comfort items

VII	Major end items and military equipment like tanks, vehicles and most Raytheon products
VIII	Medical supplies
IX	Repair parts and maintenance components
X	Material for non-military programs like economic development and disaster relief

Table 2: Classes of supply in the military [29]

Each year, the policy expands to cover a wider set of classifications as shown in Figure 3. Some products, like fuel in pipelines, cannot be physically tagged and are excluded from the policy's requirements.

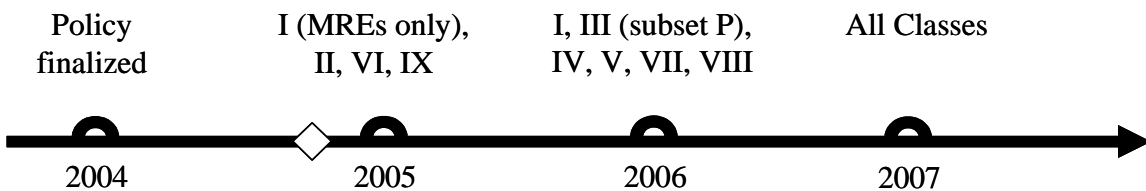


Figure 3: Commodities covered under the DoD RFID Policy

The DoD operates a large number of distribution depots in the continental U.S. and all over the world. Its contracts with suppliers stipulate that shipments are to be made to one or more of these depots. The RFID policy outlines an expanding set of depots whose shipments must be tagged, as shown in Figure 4. By 2007, all shipments to the DoD or its components (the armed forces) must have RFID tags.

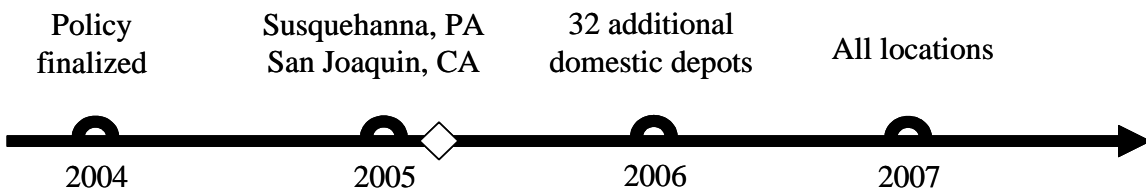


Figure 4: Depots requiring RFID tags

The third dimension along which the policy extends over time is the level of container which will require an RFID tag. Figure 5 shows how individual items are first combined into an exterior container and then loaded onto a pallet. The majority of Raytheon's shipments look like the example on the right side of the figure, where one or more shipping containers are placed on a pallet.

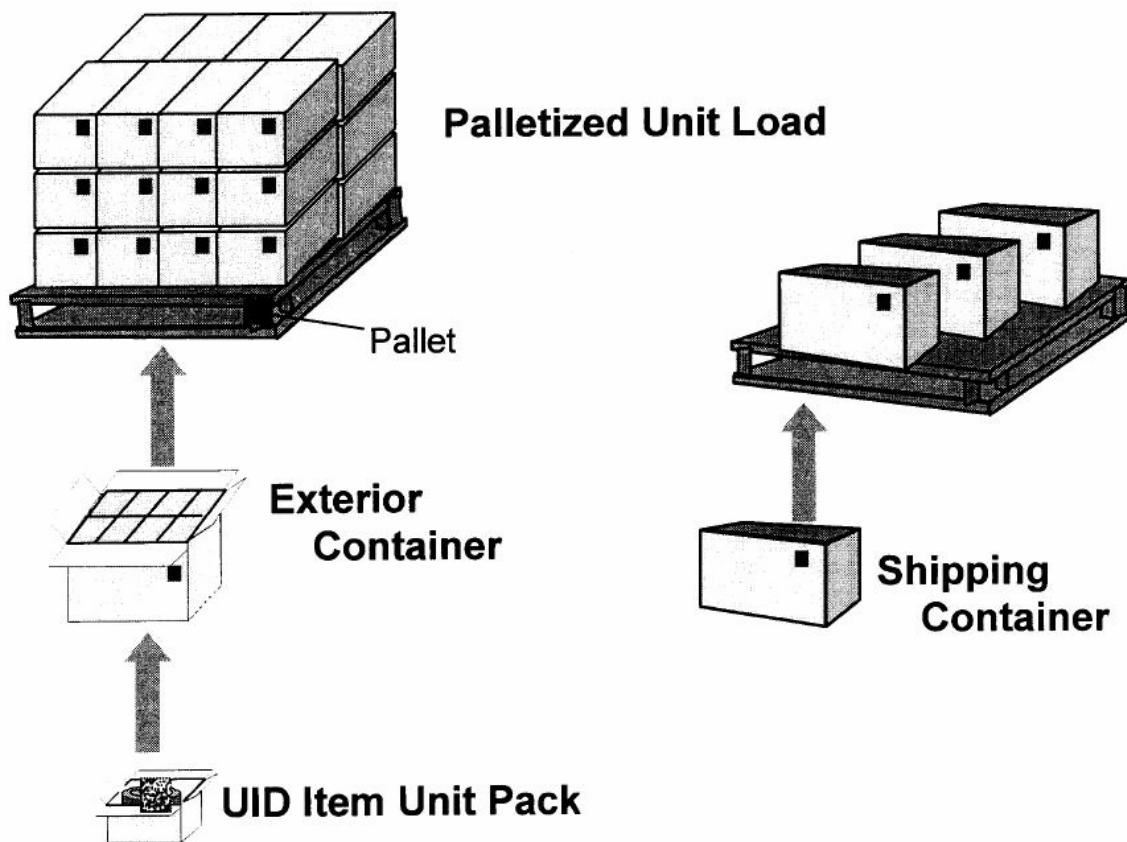


Figure 5: DoD Container Hierachy []

Before 2007, only exterior containers, palletized unit loads and shipping containers require passive RFID tags. This level of tagging is consistent with the overall goal of the RFID policy: to give the DoD visibility on items on their initial journey to the warfighter.

In 2007, the policy expands to cover “UID Item Unit Packs”. UID, or Unique Identification, is a separate policy which requires permanent serialized designations on expensive end items and repairable parts. The goal of this policy is to simplify identification and movement of product through the supply chain during the product’s entire lifecycle. The 2007 extension of the RFID policy may be the first of future attempts to reconcile these two policies.

The obvious question posed by many defense suppliers is “When will I need to be compliant?” Raytheon’s situation may be similar to others in the defense industry. The majority of shipments Raytheon makes are either spares and repair parts (Class IX) or major end items and weapon systems (Class VII). However, very few spares and repair parts are sent to either Susquehanna or San Joaquin, the commodity classifications and depots covered in the 2005 requirement. The 2006 expansion of the policy to include major end items and 32 additional depots

means that nearly all Raytheon shipments will be impacted by the policy in that year.

1.5.5.2. Workflow requirements of the RFID policy

In addition to these physical requirements, the policy also stipulates aspects of the workflow involved in transmitting RFID data. There are two components to this: The content structure of the tag's "license plate" and the transmission of data.

The policy specifies the use of EPCGlobal™ Class 0 or Class 1 passive tags. These provide either 64 or 96 bits of storage to be used for identifying the manufacturer, product SKU or Object Class, and unique serial number. The DoD accepts two formats for this information.

One is the Electronic Product Code described in section 1.5.3.1. EPCGlobal™ will make sure that manufacturers do not encroach on each others' namespaces through the assignment of globally unique EPC manager numbers. There is a membership fee associated with joining EPCGlobal™ and receiving a manager number. For many of the DoD's suppliers, this cost will be substantial in comparison with the rest of their RFID investment. It is likely that this cost would be directly or indirectly charged back to the DoD, especially if the supplier can show that it is not using RFID for other purposes.

For this reason and possibly others, the DoD has allowed the use of the "DoD Construct", an alternative namespace allocation nomenclature. It comes in several formats, but essentially allows the use of pre-existing manufacturing identifies like the Commercial and Government Entity (CAGE) code instead of EPC manager numbers [30].

Regardless of which numbering scheme is used, the supplier is responsible for maintaining rational and unique object class and serial number data. For those suppliers who also conduct business outside of the defense industry, the Electronic Product Code might make sense by eliminating the possibility of duplicate numbering schemes. All but the largest Defense-only suppliers will probably choose the DoD Construct because of its use of existing and familiar manufacturer identifiers.

Since 1999, the DoD has offered a paperless workflow system for coordinating the shipping, receiving and payments processes. This system is called Wide Area Workflow, or WAWF for short [31]. WAWF provides a clearinghouse for storing supply chain workflow documents like contracts, invoices and advanced shipping notices (ASNs). It can be accessed by all participants in the supply chain.

The RFID policy states that suppliers will use the WAWF to send advanced shipping notices to the receiving DoD entity and that the RFID tag data will be included in this ASN. The ASN transaction template will allow for RFID-specific information to be entered, including data on container and tag nesting and UID / RFID cross-references.

1.6. Primer conclusion

This chapter should provide the reader with sufficient background to understand the remaining portions of this work. The citations provide a good source of

additional information, and should be used as necessary to complement the reader's knowledge.

-
- [i] Eagle, Jim. 27 2002. RFID: The Early Years. The Eagle's Nest. 28 Dec. 2004 <<http://members.surfbest.net/eaglesnest/rfidhist.htm>>.
 - [ii] Landt, Jerry. "Shrouds of Time - The History of RFID." AIM Global RFID Connections Feb 2002. 28 Dec 2004 <<http://www.aimglobal.org/technologies/rfid/newsletter/RFIDnews02.zip>>.
 - [iii] Overby, Stephanie. "Inside an Agile Transformation." CIO Magazine 15 Aug 2004. 29 Dec 2004 <<http://www.cio.com/archive/081504/profile.html>>.
 - [iv] Savi Technology Company History. Savi Technology. 29 Dec. 2004 <<http://www.savi.com/company/ov.company.shtml>>.
 - [v] Joint Total Asset Visibility Office Charter. Joint Total Asset Visibility Office. 29 Dec. 2004 <<http://www.dla.mil/j-6/jtav/newcharter.html>>.
 - [vi] Estevez, Alan. "RFID Goes to War." CNet News.com. 22 Mar 2004 <http://news.com.com/RFID+goes+to+war/2008-1006_3-5176246.html>
 - [vii] Coyle, Edward. "DoD RFID Policy: Leading the Way in Two Worlds: Active and Passive RFID." Raytheon Enterprise RFID Kick-Off. , Waltham Woods, Massachusetts. 21 July 2004.
 - [viii] Cole, Peter. "A Study of Factors Affecting the Design of EPC Antennas and Readers for Supermarket Shelves." 1 Jun. 2002. Auto-ID Centre, University of Adelaide. 29 Dec. 2004 <<http://archive.epcglobalinc.org/publishedresearch/ADE-AUTOID-WH-001.pdf>>.
 - [ix] Scharfeld, Thomas, "An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design" (M.S. thesis, Massachusetts Institute of Technology, 2001), pp. 27 - 34.
 - [x] Finkenzeller, Klaus. RFID Handbook. 1st ed. : John Wiley & Son, Ltd., 1999, pp. 108 - 109
 - [11] Chappell, Gavin, Lyle Ginsburg, Paul Schmidt, Jeff Smith, and Joseph Tobolski. "Auto-ID on the Line: The Value of Auto-ID Technology in Manufacturing." 01 Feb 2003. 03 Feb 2005.
 - [12] Byrnes, Jonathan. "Are You Aiming Too Low with RFID?." Harvard Business School Working Knowledge 03 May 2004. 06 Feb 2005 <<http://hbswk.hbs.edu/item.jhtml?id=4107&t=dispatch>>
 - [13] Cantwell, Brian. "Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies." 01 Nov 2002. 08 Feb 2005.

-
- [14] Spychips: RFID Privacy Website. Consumers Against Supermarket Privacy Invasion and Numbering. 08 Feb. 2005 <<http://www.spychips.com/>>.
- [15] Kantor, Andrew. "Tiny transmitters give retailers, privacy advocates goosebumps." USA Today 19 Dec 2003. 08 Feb 2005 <http://www.usatoday.com/tech/columnist/andrewkantor/2003-12-19-kantor_x.htm>
- [16] History of EPCglobal US. EPCGlobal. 08 Feb. 2005 <<http://www.epcglobalus.org/About/history.html>>.
- [17] Frequently Asked Questions about EPCGlobal. EPCGlobal. 09 Feb. 2005 <<http://www.epcglobalinc.com/about/faqs.html#1>>.
- [18] Frequently Asked Questions about EPCGlobal. EPCGlobal. 09 Feb. 2005 <<http://www.epcglobalinc.com/about/faqs.html#7>>.
- [19] Floerkemeier, Christian, Dipan Anarkat, Ted Osinski, and Mark Harrison. "PML Core Specifications." 15 Sep 2003. 09 Feb 2005 <http://www.epcglobalinc.com/standards_technology/Secure/v1.0/PML_Core_Specification_v1.0.pdf>.
- [20] Mealling, Michael. "EPCGlobal Object Name Service (ONS) 1.0." 15 Apr 2004. 09 Feb 2005 <http://www.epcglobalinc.com/EPCglobal_ONS_1.0.pdf>.
- [21] Roberti, Mark. "Intermec Withdraws IP Licensing Plan." RFID Journal 03 Feb 2005. 09 Feb 2005 <<http://www.rfidjournal.com/article/articleview/1387/1/1/>>
- [22] Guidelines on EPC for Consumer Products. EPCGlobal. 09 Feb. 2005 <http://www.epcglobalinc.com/public_policy/public_policy_guidelines.html>.
- [23] EPIC RFID Privacy Page. 08 Feb. 2005. Electronic Privacy Information Center. 09 Feb. 2005 <<http://www.epic.org/privacy/rfid>>.
- [24] Action Groups. EPCGlobal. 09 Feb. 2005 <http://www.epcglobalinc.com/action_groups/action_groups.html>.
- [25] Auto-ID Labs - About the Labs. Auto-ID Labs. 09 Feb. 2005 <<http://www.autoidlabs.org/aboutthelabs.html>>.
- [26] Byrnes, Jonathan. "Who Will Profit From Auto-ID?" Harvard Business School Working Knowledge 01 Sep 2003. 15 Feb 2005 <<http://hbswk.hbs.edu/item/jhtml?id=3651&t=dispatch>>
- [27] Wynne, Michael W. Radio Frequency Identification (RFID) Policy. 30 Jul. 2004. Department of Defense Automatic Identification Technology Office. 15 Feb. 2005 <[http://www.dodait.com/rfid/RFID%20Frequency%20Identification%20\(RFID\)%20Policy.pdf](http://www.dodait.com/rfid/RFID%20Frequency%20Identification%20(RFID)%20Policy.pdf)>.

-
- [28] Wynne, Michael W. Radio Frequency Identification (RFID) Policy. 2 Oct. 2003. Department of Defense Automatic Identification Technology Office. 15 Feb. 2005 <<http://www.dodait.com/docs/Wynne%20Policy%20Memo.pdf>>.
- [29] Lai, Elaine M., "An Analysis of the Department of Defense Supply Chain: Potential Applications of the Auto-ID Center Technology to Improve Effectiveness" (B.S. thesis, Massachusetts Institute of Technology, May 2003), p. 18.
- [30] CAGE FAQ. 16 Aug. 2004. Defense Logistics Information Service. 15 Feb. 2005 <http://www.dlis.dla.mil/CAGESearch/cage_faq.htm>.
- [31] WAWF Functional Information. Wide Area Workflow. 16 Feb. 2005 <<https://wawf.eb.mil/FuncInfo.html>>.