Basic Concepts in RFID Technology

By Richard Moscatiello

Introduction

This paper explains the basic concepts of RFID technology. The presentation is (hopefully) in an easy-to-understand format. Topics discussed are as follows:

- Advantages of RFID
- Basic Concept
- Radio Waves
- Modulation
- RFID Tags
- RFID Tag Data Format
- Roll Call (Anti-collision Algorithm)
- Regulatory Environment
- You say 'Antennae', I say 'Antennas'... (Transmission Antennas)
- Making a Business Case for an RFID System

Advantages of RFID

RFID has distinct advantages over the barcode. **For example,**

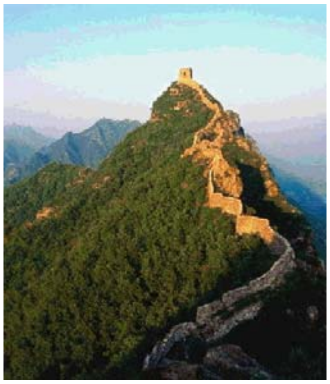
- Human intervention is required to scan a barcode, whereas in most applications an RFID tag can be detected "hands off."
- Barcodes must be visible on the outside of product packaging. RFID tags can be placedinside the packaging or even in the product itself.
- You must have "line of sight" to read a barcode. RFID tagged items can be read even if they are behind other items.q The readability of barcodes can be impaired by dirt, moisture, abrasion, or packaging contours. RFID tags are not affected by those conditions.
- RFID tags have a longer read range than barcodes.
- RFID tags have read/write memory capability; barcodes do not.
- More data can be stored in an RFID tag than can be stored on a barcode.

Note also that RFID data, once acquired, is easily managed by legacy software infrastructures implemented for the purpose of barcode inventory control and supply chain management. IT migration from barcode to RFID is virtually seamless. It is even possible to simultaneously manage RFID data and barcode data on the same platform applications.

Recently, RFID implementation has experienced an annual growth rate of 24%. Since the year 2000, rapid growth in the market for RFID is creating the economies of scale necessary to bring costs down to the point where RFID tags will soon be competitive with printed barcodes. .

In addition, there are revolutionary new fabrication techniques that further reduce costs. (See Forecasting the Unit Cost of RFID Tags).

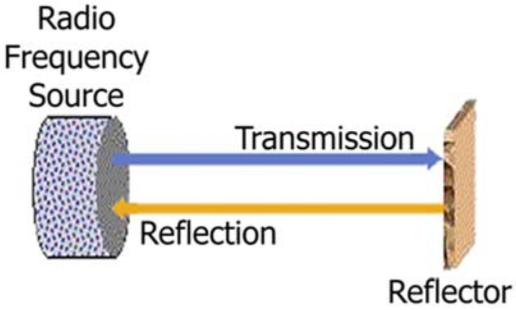
Basic Concept



The easiest way to understand RFID is to think of signal mirrors. For centuries we've known how to communicate messages with just a mirror by flashing the sun's reflection in the direction of the recipient. The flashes are sequenced to represent a code known by the recipient, for example Morse Code, that communicates intelligence without the necessity of an infrastructure that establishes physical contact (for example, a telegraph line). So, messages can be sent through the air simply by reflecting radiated sunlight. That is the basic idea behind RFID, except that instead of using radiated sunlight as our communication medium, we reflect radio waves.

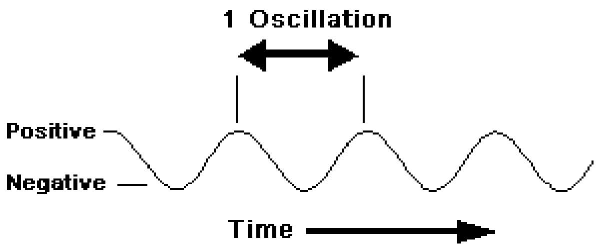
The basic theory underlying RFID technology has been understood since the 1930s. Early on it was discovered that the introduction of a conductive material into an electric or magnetic field could alter the field's characteristics. That occurs because the conductive material both absorbs and reflects the energy in the field. If the field is a radio frequency, or RF, the conductive material is capable of imparting a reflection of the source field radiation.

RFID technology takes advantage of that characteristic by manipulating the sequence and rate at which that reflection occurs, called modulation. RFID tags are designed to deliberately reflect the source RF in sequences that are interpreted as information in the form of digital data.

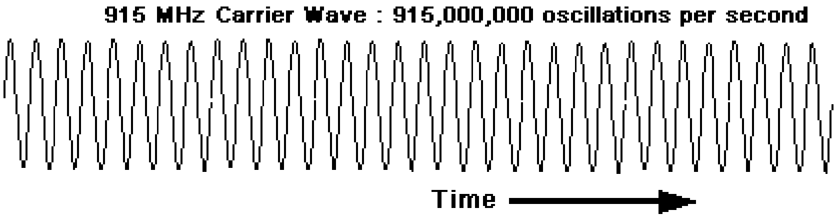


Radio Waves

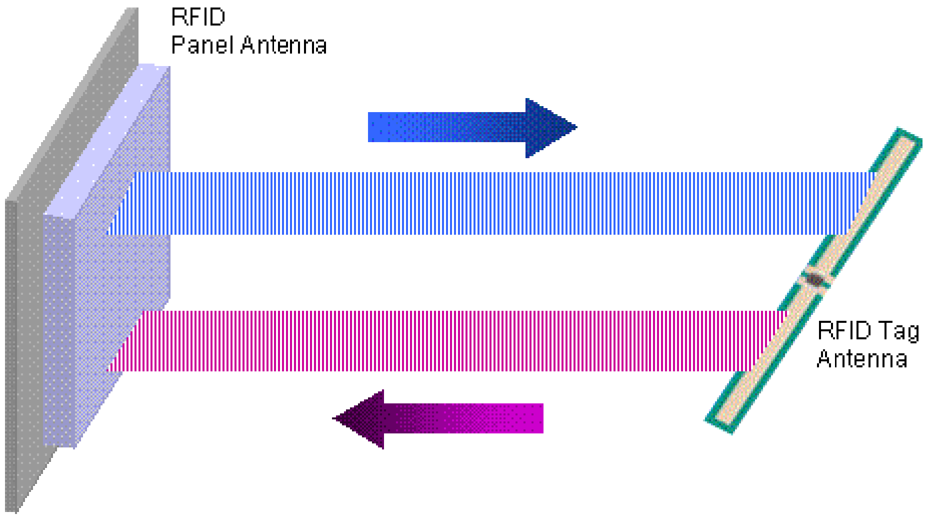
Light, X-rays, and radio waves are all *electromagnetic* waves. The only difference between them is the frequency at which the wave oscillates between positive and negative polarity. The number of waves that occur in one second is known as the *frequency*, and is measured in Hertz. One Hertz is one wave oscillation per second



RFID systems operate at a number of specified *frequency bands*. A frequency band is a range of frequencies that are close to a nominal ceter frequency. For example, the 915Mhz frequency band includes all the frequencies starting from 902MHz to 928MHz, which are subdivided into 50 communication *channels*. Some common RFID frequency bands are 125 KHz (125,000 Hertz), 13.56 MHz, 868 MHz (in Europe), 915 MHz, and 2.45 GHz (2.45 billion Hertz). Each band has it's own performance trade-offs.This tutorial focuses on 915 MHz (that's 915 Mega Hertz or 915 million oscillations per second), but the principles are basically the same for other RFID frequencies.



The channel frequency (e.g. 915 MHz) over which an RFID system communicates data is called a *carrier wave*, so called because it is used to carry dataRFID tag antennae are tuned to resonate only to the specified band of carrier frequencies that are centered on the designated RFID system frequency. Within that range of frequencies the RFID tag is able to absorb and reflect energy back to the source.

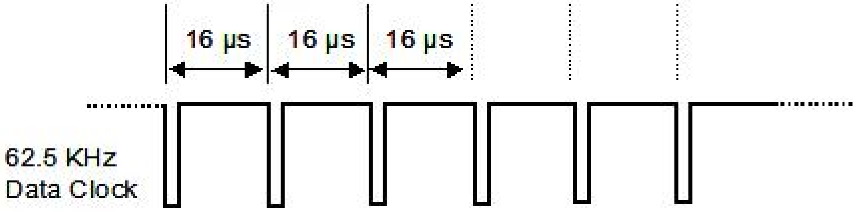


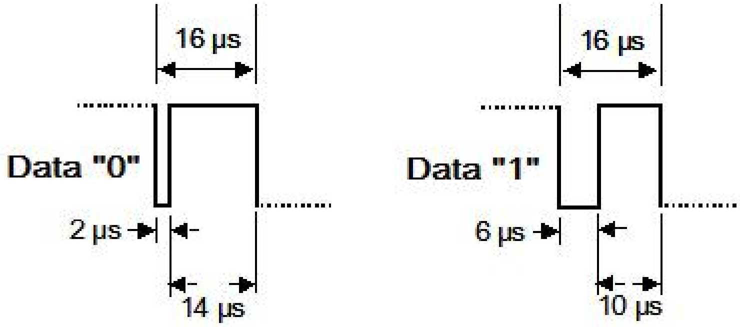
Note that the carrier wave by itself is not data, but is used to carry the data to and from the RFID tags. In order to carry data the carrier wave must be **modulated.**

Modulation

Data are communicated on an RF carrier wave via a process called modulation. In this process a stream of data pulses ("1"s and "0"s) are added to (mixed with) the carrier wave.
The data stream has a clock frequency that is much slower than the carrier wave frequency. For a 915 MHz system the data clock rate is 62.5 KHz, that is one clock pulse every 16 microseconds. The data clock will serve to synchronize the RFID tag with the RFID interrogator. There will be a data pulse every 16 microseconds.

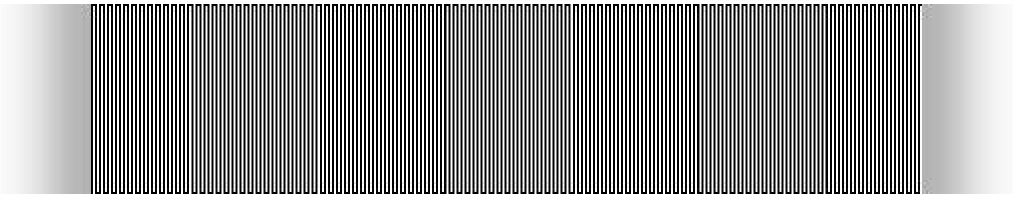
Data pulses that are 2 microseconds wide will be interpreted as data bit "0"s and pulses 6 microseconds wide will be interpreted as data bit "1"s to make the data stream.



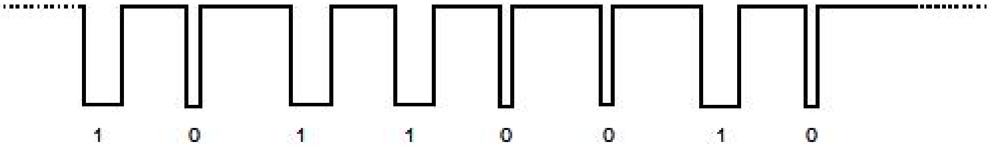


There are two types of modulation: Amplitude Modulation (AM) and Frequency Modulation (FM). Amplitude modulation works by using the data stream to vary the signal strength of the carrier wave.

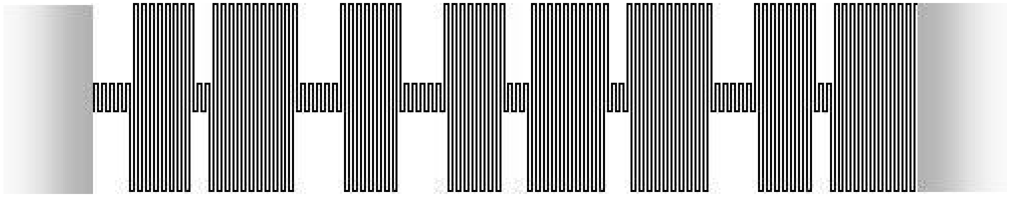
915 MHz Carrier Wave



+ Data Stream

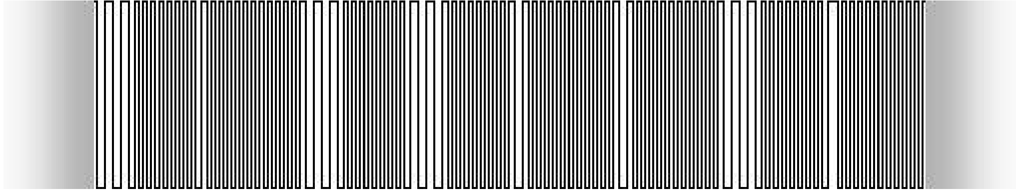


= Amplitude Modulation



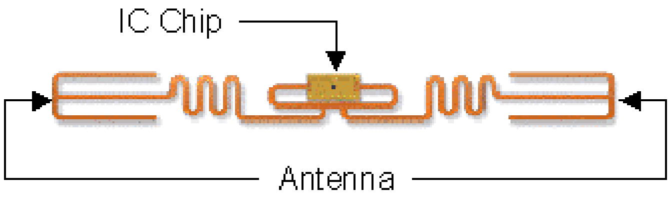
The **frequency modulation (FM)** method keeps signal strength constant and instead works by varying slightly the frequency of the carrier wave. Adding the data stream to the carrier wave would look like this:

915 MHz Carrier Wave + Data Stream = Frequency Modulation



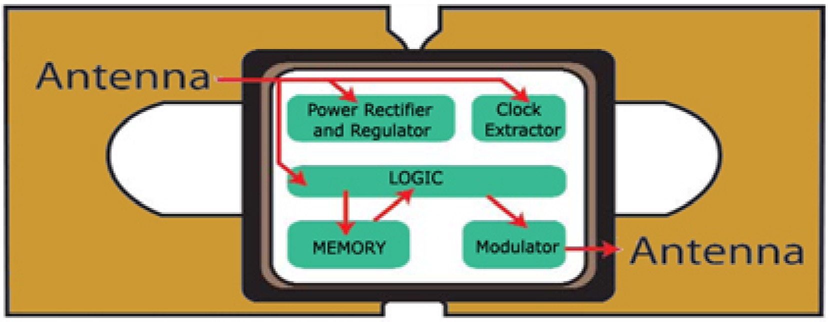
RFID Tags

In its basic form, an RFID tag consists of a silicon integrated circuit (an "IC Chip") connected to a small antenna.



There are two general categories of RFID tags, *passive tags* and *active tags*. The most common of these is a "passive" tag (shown above), so-called because it has no internal battery power. Instead, passive tags are powered by energy drawn from the RF carrier wave transmitted by the interrogator.

The modulated carrier wave transmitted by the interrogator is sensed by the **Antenna**. The carrier wave induces a small alternating current (AC) in the **Antenna.** Inside the IC Chip a **Power Rectifier and Regulator** converts the AC to stable DC and uses it to power the IC chip, which immediately "wakes up". The **Clock Extractor** separates the clock pulses from the carrier wave and uses the pulses to synchronize the **Logic, Memory,** and **Modulator** sections of the tag's IC chip with the Interrogator**.**



The **Logic** section separates the 1's and 0's from the carrier wave and compares the data stream with its internal program to determine what response, if any, is required. If the **Logic** section decides that the data stream is valid, it accesses the **Memory** section for the chip's unique identification data and any user data that have been stored there. The **Logic** section encodes those data using the Clock Extractor pulses. The encoded data stream is input into the **Modulator** section. The **Modulator** mixes the data stream with the carrier wave by electrically adjusting the reflectivity of the antenna at the data stream rate, similar to the way one might adjust the angle of a signal mirror to reflect the sun's light. Electrically adjusting the antenna characteristics to reflect RF is referred to as ***backscatter*** .

RFID Tag Data Format

Printed barcode labels generally conform to the Universal Product Code standard (UPC) of product identification. RFID tags used to identify products in the supply chain serve the same purpose, so it's often expeditious to explain RFID tags simply as "electronic barcodes." Both RFID tags and barcode labels digitally convey information about objects. Currently, "Class 1+" RFID tags are available with a digital memory of 96 bits, each bit being either a logic 1 or a logic 0. Because alphanumeric characters (i.e., A-to-Z and 0-9) each require 8 bits of memory, it's possible to store 12 characters in an RFID tag (which isn't saying much). On the other hand those 96 bits represent a possible **79,228,162,514,264,300,000,000,000,000** (that's over **79.2 trillion trillion**) unique numerical identities. Or you could split the 96 bits into fields that each represent some characteristic of the object, creating a sort of family tree of objects.

There are two basic tag data architectures. One is to include all information about a product (e.g., its size, date of manufactures, the quality inspector's name) on the tag itself. This has the advantage of decentralizing the data, but has a drawback in that the increased memory requirements on the tag increase its complexity and cost. The other way is for the tag to serve as a "license plate" for the object, that can be associated with a database of its characteristics located in a centralized database.

In 2000, Sarma, Brock, and Ashton of MIT's Auto-ID Project foresaw a world where *"all physical objects…act as nodes in a networked physical world."* [1] They propose an open architecture system that is independent of the specific tag technology affixed or built into the object being tracked. They proposed a common identification standard or Electronic Product Code (ePC) standard.

Source: Sarma, Brock and Ashton

The header serves as a way of identifying the format of the sequence of bits that follow in the EPC. This makes system coding more flexible. That is a critical innovation because it allows for the use of various independent standards of identification to be understood by users of other formats. Sarma, et al suggested an Object Name Service (ONS) organization for registering and tracking product names, similar to the Domain Name Service (DNS) that registers web-site names. [2]

Roll Call

Imagine for a moment a room full of tagged objects interrogated by an RFID reader. What happens if all the tags respond simultaneously? There would be on unreliable cacophony of responses, similar to a data-bus crash in a computer. The fact is, our hypothetical room-full of tags will indeed all try to reply at roughly the same time, and the resulting data crash is one of the critical technical hurdles RFID technology has had to surmount. The solution is referred to as an *"anti-collision"* algorithm.

A small population of tags can be read in 2.5 milliseconds. A large population of tags will require the reader software to perform a slotted random anti-collision algorithm whereby the reader assigns a pseudo-random number into each tag's slot counter which each reply when their slot counter reaches zero. This prevents all of the tags from replying at the same time. Acquisition time will increase based on the number of tags in the field of view.

The following explanation was authored by Benny Martinez of Los Alamos National Laboratories:

> "Each Tag within Interrogator range becomes engaged with the Interrogator in a pseudo-random sequence to allocate its response time slot. When the initial Interrogator query is made, all of the Tags within range will reply. Because collisions are unavoidable when more than one tag is in the field of view, Tag replies are managed through a "slotted

---

[1] Sarma, Sanjay; Brock, David L.; Ashton, Kevin, The Networked Physical World, MIT-AUTOID-WH-001 (Massachusetts Institute of Technology, 2000) page 4

[2] Sarma, Sanjay; Brock, David L.; Ashton, Kevin, The Networked Physical World, MIT-AUTOID-WH-001 (Massachusetts Institute of Technology, 2000)

> ALOHA" communications protocol. The Interrogator provides a variable number of random time-slots for individual tags to reply in, with the number of slots being determined by the number of initial collisions detected, i.e. by the number of tags present. The interrogator identifies each Tag that stands out among the cacophony of collisions, allocates it a slot and silences each one it identifies. The number of slots can vary from 8 to 1024. The Interrogator starts by assuming there are 8 tags, but if after filling these slots [if] more Tags are responding, it increases the number of slots by an order of magnitude. The Interrogator continues requesting responses until no further collisions are detected, (i.e. the Interrogator has identified and slotted all the Tags within range). The maximum of 1024 slots was chosen as a tradeoff between frequency band "on" time and number of Tags expected to be within range of the Interrogator but that maximum could be raised, recognizing there would be concomitant increases in frequency band "on" time.
> ...Anti-collision protocols...allow multiple readings of tags simultaneously present in the field of the antenna. Such reader/writers can successfully read 20 to 50 [citation] tags in one second, depending on site configuration and tag protocol. Aside from that, memory capacity and time are the only other constraints."
>
> [citation] AIM Inc. Frequency Forum White Paper v1.0, 2000-07, Draft Paper on the Characteristics of RFID-Systems Text courtesy B. Martinez

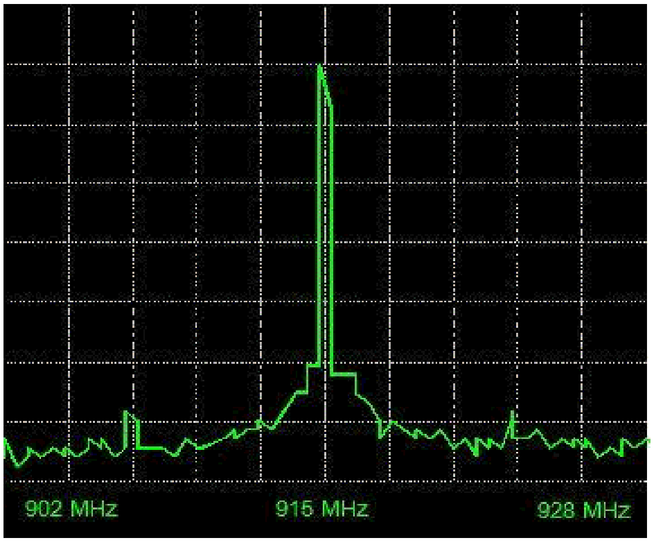
Regulatory Environment

Federal Communications Commission Title 47 Part 15 regulates radio frequencies in order to prevent interference with other electronic communication systems at or near the same frequency bands.

The RFID "915 MHz frequency band" is actually a range of carrier frequency *channels* extending from 902 MHz to 928 MHz.

Regarding RFID operation in the 915 MHz frequency band, FCC Section 15.245 limits 902 MHz to 928 MHz to a field strength of 1/2 volt per meter measured at 3 meters. **That has important implications with regards to the *read range* of your RFID tags. Optimization of tag readability is a crucial design consideration in your RFID system integration plan.**

Section 15.247 further stipulates that the RFID carrier frequency must "hop" from channel to channel within the 902 MHz to 928 MHz bandwidth. The regulation specifies 50 channels, and the RFID interrogator may not dwell on any channel for more than 4 tenths of a second before switching to another channel.



The RFID interrogator hops to "channel frequencies that are selected at the system hopping rate from a pseudo-randomly ordered list of hopping frequencies." Channel synchronization with the RFID tag is simple: the RFID tag antenna is designed to pick up any frequency in the 902-928 MHz band, and merely reflects whichever frequency channel the interrogator is transmitting on at any particular time.

You say 'Antennae', I say 'Antennas'...

The choice of interrogator antenna is influenced by the intended application. Antennas each have unique characteristics that benefit specific uses. The primary characteristics are:

- polarization
- beamwidth (directionality)
- gain
- dimensions (form factor)

Antenna **polarization** refers to the orientation of the carrier wave as it travels through space. Antennae may have linear polarization or circular polarization . This is important as it relates to the orientation of your RFID tags on the asset being tracked.

Linearly polarized antennae radiate in only one plane. If the interrogator antenna and tag antenna are both linearly polarized *and* if the two antennas are at right angles to each other, the tag will not be read. If the tag is parallel to the reader it *will* be read. However, the advantage of linearly polarized reader antennas is that they concentrate transmit power on the same plane, whereas circularly polarized antennas distribute power over a 360 degree cycle. So, if it is known that linear tags will always be in the same orientation (for example, on a product packaging conveyor) a Linear reader antenna may be the preferred choice for better performance.

A Circularly polarized antenna cycles its electric field through 360 degrees and will read tags that are designed with either linear polarization or circular polarization characteristics. Circular antennas will read tags from just about any angle with respect to the interrogator antenna. That's an advantage where tagged items of different shapes, sizes, and orientations are being interrogated by the reader.

The **half-power beamwidth** defines the anglular spread of the transmitted carrier measured from the antenna to the point where signal power has dropped by 50% (or 10 decibels). A wider beamwidth divides its power over a greater area, increasing the spatial envelope in which a tag can be read, but at the cost of decreased linear range. Conversely, a narrow beamwidth has the advantage of increased range and a limited angular window in which to read a tag. Note that there are null spots directly in front of, and to the sides of, a typical antenna. In order to optimize reads, an effective RFID system will be designed such that the average distance to a tag is neither too close nor too far away from the antenna. For a 915MHz system using a circularly polarized panel antenna, that is approximately 3 to15 ft, and with an angular offset from the antenna center line that does not exceed the half power beam width of the antenna.

Antenna **gain** refers to how much signal power is input to the antenna (from the reader unit) compared to how much power is transmitted from the antenna. Gain is a consideration with respect to FCC regulatory conformance.

Form factor is, quite simply, the dimensional constraints imposed on the RFID system by its operating environment. In other words, will the antenna fit into the space available?

Making a Business Case for an RFID System

The purpose of an RFID system is to save money, so it's important to quantify that to justify the cost. The following is an excerpt from a proposal for an IV Pump tracking system at a major US hospital.

By far the pivotal benefit will be the shift from “random discovery” of units into “targeted visibility” of units. The system is an inexpensive, practical system that can be deployed quickly, is easy to use, and is scalable to future needs.

Staff in clinical, maintenance, medical engineering, and financial areas will benefit from instant position information, usage analysis, etc.

Analysis tools from the project will ensure that expansions are directly related to specific needs and to definable financial savings or gains.

Data obtained in 2004 provided a baseline for estimating the value of the proposed RFID system. The hospital owns about 600 IVPs for which MVS has a complete data set. Although there are more items in the mix of items to be tracked, focusing on these 600 IVPs provide a conservative baseline for evaluating the financial impact of the tracking system.

Hospital DME List

Anesthesia and Pumps	Units per yr.	Cost per unit	% Missing	Annual Unit Loss
Single Channel Pumps	400	$ 4,000	15-20%	3-4/year
Triple Channel Pumps	200	$ 6,500	15-20%	3-4/year

The data also tell us that the hospital rents 20-25 IVPs per year to cover for units missing (temporarily invisible) or lost (non-recoverable). IVP rental costs are given as $1000 per month. Keeping with a conservative interpretation of cost/benefit, assume 15% Missing and six IVPs unrecoverable per year. Assuming a 5-year straight-line depreciation of those assets, the 15% Missing represent a loss of use of those items of …

Single Channel Pumps: (400 x $4000 x .15) /5 =	$48,000
Triple Channel Pumps: (200 x $6500 x .15) /5 =	$39,000
Add the replacement cost of the 6 non-recoverable units…	
Single Channel Pumps: (3 x $4000) =	$12,000
Triple Channel Pumps: (3 x $6500) =	$19,500
And…	
IVP Rental costs: (12 months x $1000 =	$12,000
Total	**$130,500**

Therefore the asset loss impact traceable to the current "random discovery" method of IVP management is about $130,500 annually.

Now consider the value of the MVS RFID system. Assume that the RFID "targeted visibility" method results in a modest 25% improvement in asset recovery and redistribution costs, an annual savings of $32,625. Applying the same 5-year depreciation to the RFID system cost of $109,665 returns an annual RFID cost of $21,933. Add the annual ASP subscription cost of ($600 x 12 months=) $7200 for a total of $29,133 per year, resulting in a net annual savings of $3492 after the cost of the RFID system is deducted. However, a 25% reduction in asset costs is a worst-case scenario. A 50% improvement is to be expected. To summarize…

Percentage of improvement	25%	50%	75%
Savings	$32,625	$65,250	$97,875
RFID system cost	$(29,133)	$(29,133)	$(29,133)
Net Annual Savings	**$3,492**	**$36,117**	**$68,742**

After the RFID system is fully depreciated in 5 years, and assuming no growth in the number of items being tracked, annual system cost drops to $7200.

Percentage of improvement	25%	50%	75%
Savings	$32,625	$65,250	$97,875
RFID system cost	$(7,200)	$(7,200)	$(7,200)
Net Annual Savings	**$25,425**	**$58,050**	**$90,675**

The above cost analysis does not take into consideration several additional factors, difficult to quantify, that are nonetheless significant contributors to the bottom line. Among those factors are…

- Reducing the Float of High Value Equipment
- Minimizing Rentals
- Fewer Equipment Purchases
- Increasing Nursing Staff Patient Care Time
- Productivity improvement of equipment distribution employees
- Higher Retention of Staff (estimated savings of $300k/Annually)
- On-time scheduled maintenance and certification of medical equipment
- Lowering costs associated with JHACO audits

Furthermore, MVS predicts that new visibility of IVP usage patterns will result in identifying available process efficiencies that are currently hidden from view.