A Primer on RF Communications and RF Tags

Almost everything you thought you wanted to know and were not afraid to ask

Michael Lind and Curt Carrender
Pacific Northwest National Laboratory, Richland, WA
November 1999

General Background Information

In the interest of time, this brief introductory paper has been liberally plagiarized from numerous internet sources and interspersed with personal experience data. It is not intended to be a definitive resource on the topic, but rather a quick reality check. My apologies to the original authors for not crediting their work from which much of this document was excerpted.

Before embarking on a detailed discussion of RF Tag technology, an understanding of the general context of RF communications is presented. The table below illustrates some of the most common communications bands, modulation techniques and standards. Licensing requirements and applications vary throughout the world.

Common Frequency Bands and Applications

125 KHz	RFID
170 - 190 kHz	LF band radios Beacons
550 - 1600 kHz	AM broadcast communications Low power voice and data
13.56 MHz	RFID
27 MHz	CB radios Low power voice and data
49 MHz	Cordless telephones Low power voice and data
88 - 108 MHz	FM radios Low power voice and data
150 - 170 MHz	Commercial two-way voice , Pager services
260 - 470 MHz	303 MHz garage door openers 433 MHz RFID Keyless entry systems Security alarms
824 - 849 MHz	Cellular phones
869 - 894 MHz	Cellular phones

902 - 928 MHz	915 MHz RFID ISM band Wireless LAN's Part 15 devices (spread spectrum cordless phones, etc.) Military radio location systems Federal mobile communications
930 MHz	Pager services with high transmitter power
2.4 - 2.4385 GHz	Amateur satellite Part 15 devices Microwave ovens and systems Army packet radio development
2.45 MHz	RFID Bluetooth
5.727 - 5.875 GHz	Amateur satellite Part 15 devices Naval radar systems Test range instrumentation radars RFID
24 - 24.25 GHz	Radio navigation

Modulation techniques

Like carrier frequency, modulation techniques vary with the application. Modulation is a technique in which a carrier wave is used to carry information from one place to another. The carrier sine wave is modified in either amplitude, phase, or frequency, so that the information is present on the wave, and can be decoded at the receiving end. Historically, commercial radio frequency applications have relied on narrow band transmission, where signals are broadcast over a narrow portion of the radio spectrum at specific frequencies which are licensed to users by the Federal Communications Commission (FCC). Most licensed narrow band systems in the U.S. operate at 25 KHz bandwidth, in the 450 MHz to 470 MHz frequency range at a speed of up to 19.2K bit per second (bps). Narrow band has been and continues to be the transmission method of choice for large, single-site industrial applications because of its consistent system performance and coverage combined with protection from interference offered by FCC licensing. The three major types of digital modulation are amplitude shift keying (ASK), phase shift keying (PSK), and frequency shift keying (FSK).

ASK is rarely used in wireless applications because multi-path effects can dramatically influence the amplitude of the information-bearing signal. This causes errors when the signal is received and decoded. PSK and FSK, on the other hand, are more common in wireless systems because of their robustness in the presence of multi-path.

There are many hybrid forms of ASK, PSK, and FSK. For example, Binary Phase Shift Keying (BPSK) is a form of PSK in which only two phase states are allowed. It is highly robust to multi-path propagation, but is not used in high data rate applications because it is bandwidth inefficient.

Other forms of PSK, such as Quadrature PSK (QPSK) allow for more phase states, thereby providing greater spectral efficiency at the cost of more susceptibility to multi-path.

One special form of modulation that has actually become a buzzword in the wireless industry is spread spectrum. Spread spectrum and many other hybrid techniques are used in some of the major cellular and data networking standards. Spread spectrum is a special modulation technique that spreads the transmitted signal over a frequency range much wider than the minimum bandwidth required to send the signal. Widening the signal bandwidth in this fashion increases the probability that received information will closely match the transmitted information. Spread spectrum transmission offers about one-quarter the coverage (compared with narrow band transmission) per base station, but on the other hand, it offers faster baud rates of 2 Mbps. Spread spectrum systems also offer more flexibility for small, multi-site, and global applications, because they don't require FCC licensing.

Spread spectrum radio technology was originally developed during World War II for covert radio transmissions. It provides immunity to interference by broadcasting redundant data across a broad range of frequencies within the unlicensed 902 MHz to 928 MHz, 2.4 GHz to 2.48 GHz, or 5.725 GHz to 5.850 GHz bands; or by continually changing frequencies within those bands. Spread spectrum transmission development in the AIDC industry began with the 900 MHz band, using a technique called direct-sequence modulation to spread the signal over a range of channels. Each data bit is transmitted over at least 10 different channels for redundancy, and the spread spectrum receiver decodes the binary data and reconstructs it into the original bit stream. Transmitting over an extended bandwidth results in quicker data throughput, but the tradeoff is diminished range.

Many spread spectrum networks, particularly those operating in the internationally sanctioned 2.4 GHz range, use frequency hopping rather than direct-sequence techniques to spread the signal over the radio spectrum. With frequency hopping, the radio transmits short bursts of data, skipping from frequency to frequency. Frequency hopping can overcome interference better than direct sequencing, and it also offers greater range (though still not the degree of range offered by narrow band transmission). This is because direct sequencing uses available power to spread the signal very thinly over multiple channels, resulting in a wider signal with less peak power. In contrast, the short signal bursts transmitted in frequency hopping have higher peak power, and therefore greater range.

When it comes to protection from interference, users of FCC-licensed narrow band systems have a regulatory edge and an avenue of redress if radio interference does occur. Spread spectrum technology is based upon interference avoidance techniques, but if some outside transmission does interfere, users can only switch to another frequency setting. These problems are more likely to occur within the heavily trafficked 900 MHz band than within the 2.4 GHz band.

Wireless standards

Some of the major standards used to guide the development of wireless communications are listed below along with a statement of their scope. Most of these can be found on the internet.

IEEE 802.11 -- 802.11 is the IEEE standard for wireless LAN's. The goal of the IEEE 802.11 committee is to standardize wireless LAN development in the Industrial, Scientific, and Medicine (ISM) frequency bands that were allocated by the Federal Communications Commission (FCC) in the mid 1980's. The bands encompass the frequency ranges 902 - 928 MHz, 2400 - 2483.5 MHz, and 5725 - 5850 MHz. The advantage of the ISM bands is

that they are unlicensed. As long as a device operating in the ISM bands meets special FCC regulations, it does not require a license. Many devices operating in the ISM bands use spread spectrum modulation. However, the FCC does permit narrow band modulation techniques to be used, provided that the respective device meets stringent power requirements. The standard focuses on the media access control (MAC) and the physical (PHY) protocol levels. The IEEE 802.11 standard is still under development, but is anticipated to become the wireless LAN standard.

IrDA -- The Infrared Data Association (IrDA) was formed to develop a standard for wireless communication using infrared (IR) technology. Some of the chief goals of the committee are to develop a standard that permits low cost, low power, point-to-point user communications using IR as the transmission medium.

CEBus -- The Consumer Electronics Bus (CEBus) standard was created by the Electronic Industries Association (EIA). CEBus is an engineering standard for home automation products. It supports carrier current, RF, IR, coaxial cable, twisted pair, and eventually fiber optic cable.

AMPS -- Advanced Mobile Phone System. AMPS is the first analog cellular standard in the U.S. Although AMPS is still in use, it is anticipated that it will be replaced by the United States Digital Cellular(USDC) standard.

IS-54 -- Interim Standard 54. See USDC.

GSM -- Global System for Mobile. The GSM standard was developed in Europe to standardize cellular communications among European countries. GSM has demonstrated substantial success and is now one of the world's most popular standards for new cellular radio and personal communications equipment.

DECT -- Digital European Cordless Telephone is a universal cordless telephone standard developed by the European Telecommunications Standard Institute (ETSI). DECT offers services for both voice and data communications.

USDC -- United States Digital Cellular, also known as IS-54 (Interim Standard 54), was developed to replace the AMPS standard, particularly in urban areas where AMPS did not provide adequate channel capacity. USDC allows the coexistence of AMPS so that providers can gradually phase out AMPS as needed.

IS-95 -- IS-95 is a U.S. digital cellular standard that uses a Code Division Multiple Access (CDMA) scheme. In a CDMA system, users share time and frequency resources simultaneously. This is made possible by assigning each user a distinct digital code. This code is added to the information data and modulated onto the carrier, using spread spectrum techniques. Although IS-95 is anticipated to provide significant capacity improvement and increased interference rejection over other digital cellular standards, it remains somewhat controversial because of its wide bandwidth requirements.

CDPD -- Cellular Digital Packet Data is a digital standard for packet data services. CDPD was designed to overlay with existing cellular infrastructure, thereby permitting simple and inexpensive installation.

PHS -- The Personal Hand-phone System is a standard developed in Japan. PHS is geared specifically for indoor and micro-cell usage.

Radio Frequency Identification (RFID) Tags

A basic RFID system consist of three components:

An antenna or coil
A transceiver (with decoder)
A transponder (commonly called an RF tag) that is electronically programmed with unique

information

The antenna emits radio signals to activate the tag and read and write data to it. Antennas are the conduits between the tag and the transceiver, which controls the system's data acquisition and communication. Antennas are available in a variety of shapes and sizes; they can be built into a door frame to receive tag data from persons or things passing through the door, or mounted on an interstate toll booth to monitor traffic passing by on a freeway. The electromagnetic field produced by an antenna can be constantly present when multiple tags are expected continually. If constant interrogation is not required, the field can be activated by a sensor device.

Often the antenna is packaged with the transceiver and decoder to become a reader (a.k.a. interrogator), which can be configured either as a handheld or a fixed-mount device. The reader emits radio waves in ranges of anywhere from one inch to 100 feet or more, depending upon its power output and the radio frequency used. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer for processing.

The significant advantage of all types of RFID systems is the non-contact, non-line-of-sight nature of the technology. Tags can be read through a variety of substances such as snow, fog, ice, paint, crusted grime, and other visually and environmentally challenging conditions, where barcodes or other optically read technologies would be useless. RFID tags can also be read in challenging circumstances at remarkable speeds, in most cases responding in less than 100 milliseconds. The read/write capability of an active RFID system is also a significant advantage in interactive applications such as work-in-process or maintenance tracking. Though it is a costlier technology (compared with barcode), RFID has become indispensable for a wide range of automated data collection and identification applications that would not be possible otherwise.

RFID tags come in a wide variety of shapes and sizes. Animal tracking tags, inserted beneath the skin, can be as small as a pencil lead in diameter and one-half inch in length. Tags can be screw-shaped to identify trees or wooden items, or credit-card shaped for use in access applications. The anti-theft hard plastic tags attached to merchandise in stores are RFID tags. In addition, heavy-duty 5- by 4- by 2-inch rectangular transponders used to track inter-modal containers or heavy machinery, trucks, and railroad cars for maintenance and tracking applications are RFID tags

A typical RF Tag system will contain both *tags* and the *tag readers* or *interrogators*. There are three main categories of RFID. These are beam powered passive, battery powered semi-passive, and active. Each operates in fundamentally different ways.

The beam powered RFID tag is often referred to as a passive device. This is because it derives the energy needed for its operation from the incident radio frequency energy beamed at it. The tag rectifies this field and changes the reflective characteristics of the tag itself. The delta in reflectivity seen at the interrogator antenna between the two reflective states is the mechanism used to transmit data back to the interrogator. Tags of this type require no. Efficiency not withstanding, there is no fundamental reason an active tag could not be built which derives the energy required for its operation from the incident radio frequency energy beamed at it.

A battery powered semi-passive RFID tag operates in some ways similar to the fully passive device. It modulates its RF cross section in order to reflect a delta to the interrogator which develops the communication link. In the case of the battery powered tag, the battery is the source

for the tag's operational power; not the incident beam. In general these tags have higher cost and greater functions than their beam powered counterparts.

Finally, there is the active RFID tag. This is simply a transmitter which creates its' own radio frequency energy. In general, these have the highest function, shortest battery life and highest cost of all tags.

Further categories exist. Tags can be grouped by their capability to change information, (read vs. read-write), their frequency band, their physical size, their operational range, their data characteristics or by their cost. In general, all of these and more should be considered in choosing the correct technology for a particular application. In choosing the technology many comparisons will arise. I will look specifically at comparisons of frequency, modulation technique, range, information content, security and cost.

Frequency:

While it is technically conceivable to do RFID tags at any frequency the most common bands are 125 kHz, 13.56 MHz, 433 MHz, 915 MHz, 2,450 MHz and 5,800 MHz. Other bands may also be used for applications such as electronic article surveillance but the above covers most world usage for true RFID. In general, the customer or end user could care less what frequency band is being used. They are only interested in function. However, regional licensing issues and functionality of the various bands do make this an issue. The 6 bands are addressed separately below.

125 kHz is actually used to couple tags to the reader inductively and not via true RF, however, these tags are so often referred to as RFID tags and are similar in function. These short range tags are chiefly used for ID badge access control, asset tracking when near proximity reads are acceptable, and ear tags for animals for tracking and control. In general the range on these systems is limited to about 30 cm in the real world in spite of manufacturers claims to the contrary. RFID tags of all kinds are highly effected by their surroundings so a data sheet range number is often optimistic. To the credit of the 125 kHz tags, their range is less perturbed by their surroundings than other tags. The 125 kHz field permeates obstacles better than other, higher frequency, fields. The data rate, due to the lower carrier frequency, is lower. A lower data rate leads to a lower transaction speed. The devices themselves, being lower frequency, are able to use less sophisticated ASICs and, as such, are often less expensive. These devices can be read only, read-write, beam powered or battery powered. Physically, a large number of these tags are credit card sized, but they can be smaller if required. These tags can be formed, (somewhat larger than normal), as washers, buttons or screws for easy attachment to the tracked article.

13.56 MHz is primarily employed in Europe and Asia for fare payment and smart card type applications. These tags are less popular in the US due to licensing differences. The range on these tags is about 70 cm, but can be much less due to power level differences. These devices share many of the attributes of the 125 kHz tags with the added advantage of a somewhat higher data rate. Again, these tags can be beam powered, battery powered, read only or read-write.

433 MHz, while not a universally accepted frequency, has the advantage of a potentially higher data rate, the longest read range at over 10 meters and lower cost than the true microwave RFID tags. It is not legal in the US at extended power levels.

915 MHz was the first real success for true RFID in the higher bands here in the US. All rail cars which travel on shared lines are required to have two RFID tags, one per side, in North America.

These are beam powered, read only tags with a range of 10 meters. The advantages of the 915 band are this range, the ability to go beam powered or battery powered, and a sufficiently high data rate to allow high speed transactions to take place. Disadvantages include a relatively large tag, (less than 2 square inches of surface area is difficult), and the requirement for fairly sophisticated rectification techniques for beam powered or for tags with write capability.

2450 MHz is a band which has traditionally received more attention in Europe and Asia than here. It is legal in the US, however few applications require the smaller size tag possible at 2450. The increasingly crowded spectrum at 915 along with the need for world wide potential, (915 is illegal in Europe), has recently made this band more important in the US. 2450 tags can be beam powered at one meter range, read only or read-write. Battery powered tags at 2450 are traditionally limited to less than 10 meters, however PNNL has recently demonstrated a compliant system with up to 200 meters of range. 2450 systems typically have difficulty operating in harsh environments with clutter, as do all microwave systems with increasing frequency. These systems have high data capability and the tags can have antenna structures of less than 1 square inch. Again, as frequency increases the cost of components increase.

The 5.8 GHz band is our final RFID type. This is of primary interest for European and Japanese toll payment. Most all that applies to 2450 MHz applies to 5.8 GHz with the exception of the tags being, on the average, more expensive and lower range. The toll systems so developed have ranges of 10 meters or less when acting in a passive or semi-passive mode. By some accounts this will become a universal standard for automobile RFID. Only time will tell.

Modulation

While an active tag can potentially have any type of modulation most fall into AM, FM, or QPSK. Most passive tags, either beam powered or battery powered, are amplitude or phase modulated.

Range

Again, this is generalized. Range is as follows. LC indicates licensing concerns or country specific concerns. Active transmitter's range is often determined more by the receiver sensitivity than any physics of the band. As such the active transmitter ranges can vary the widest.

125 kHz	30 cm passive and semi-passive, no active counterpart
13.56 MHz	70 cm passive and semi-passive, no active counterpart LC
433 MHz	15 meters passive, 30 meters semi-passive, 200 meters transmitter. LC
915 MHz	10 meters passive, 20 meters semi-passive, 150 meters transmitter. LC
2.45 GHz	1 meter passive, 10 meters semi-passive, 50 meters transmitter. LC
5.8 GHz	No passive counterpart, 10 meters semi-passive, 50 meters transmitter. LC

Information content

In theory, any of these tags can have infinite data. In practice lower frequency tags (below 915 MHz) normally have 32 to 128 bits of data and higher frequency tags have up to 1 Mb of data. Generally the realistic limit is 1 kb or less for these tags. The best way to set a realistic limit is to look at data rate and true data throughput rates. 125 kHz tags can support up to 1 kHz data rates. If a transaction can take no longer than 100 ms, (such as a door opener), a 32 bit ID is about maxed out when overhead is considered. For higher speed toll applications the 2450 band and 5.8

GHz band require and can support up to 2 Mb data rates. Often however the amount of time in the field and the required overhead result in a nominal data transfer of about 2 kb for passive tags.

Security

A true discussion on security should address the prospect of privacy and anonymity as well, however most systems make these moot points. There is very little consideration to any security in any of these systems. Fully secure, (RSA encryption and spread spectrum), systems have been built but none are currently used in volume. Technically, back-scatter tags are less easily observed and back-scatter readers are more easily observed than their active counterparts. Of all systems in circulation today, none offer sophisticated security and most have it actively designed out.

Cost

The following table gives the approximate cost ranges of commercial tags

125 kHz:	$1 to $2 passive, $4 semi-passive
13.56 MHz:	$2 to $6 passive, $4 to $10 semi-passive
433 MHz:	$13 to $20 passive, $18 to $35 semi-passive, $30 to $50 active
915 MHz:	$5 to $40 passive, $20 to $60 semi-passive, $30 to $50 active
2.45 GHz:	$5 to $40 passive, $20 to $200 semi-passive, $50 to $100 active
5.8 GHz:	$40 to $300 semi-passive, $80 to $300 active.

Communications Network Architecture

A logical and often necessary adjunct to the RF tag architecture is joining multiple tags together into a network. Although "open system" standards are in the works, vendors of RFDC systems within the AIDC marketplace currently offer proprietary networks using their own dedicated equipment. However, all radio frequency local-area networks (LANs) follow roughly the same architecture.

The most common approach to radio frequency implementation uses wireless terminals (either handheld or vehicle-mounted) that include a radio transmitter/receiver, keyboard, LCD display, and usually a barcode scanner. The terminals communicate with the master radio transceiver, a.k.a. base station or wireless gateway, which receives and routes messages from the individual terminals to the radio frequency network controller, and also routes messages such as instructions and exceptions from the host system to the terminals.

The base station receives data from the terminals by means of polling or contention protocols. With polling, each radio frequency terminal is polled or queried in a specific sequence. In a contention system, each terminal transmits on its own accord; if the channel is busy, the terminal retransmits after a randomly set delay. The polling method is preferred for systems with few terminals and approximately uniform transaction rates. Systems with many terminals and high transaction rates achieve more consistent response rates with the contention method.

The radio frequency network controller (which may be a PC) acts as the interface between the radio network and the host computer and/or data collection program. The controller/PC may

interface via wire with an autonomous host, or the PC may itself be the host with the data collection program/database resident on it.

Because of the possibility of electromagnetic and other radio signal interference within a facility, the placement of the antenna and base station(s) as well as other system components is critical to system performance; a professional site survey is highly recommended. Depending upon the size and layout of a facility, repeaters and/or multiple base stations may be required to assure complete radio coverage.

Terminal emulation is the most common means of host connectivity, where emulation software, running on both the terminals and the network controller, makes the radio frequency terminals appear to be standard terminals acceptable to the host, resulting in a quick and easy host connection.

However, the latest generation of radio frequency devices uses a client/server approach, where each individual terminal uses a network driver, giving access to the network so it can communicate directly with the host or any other application. The client/server architecture provides extremely fast response rates, because the data collection program doesn't have to run on the host as it does with terminal emulation (with client/server RFDC, the host is only used for look-ups and updates, considerably reducing transaction traffic).

Where a radio frequency local area network (LAN) may cover a 50,000 to 1,000,000 square-foot facility, a radio frequency wide area network (WAN) can cover entire geographical regions. With radio frequency WANs, network operations are managed by vendors (ARDIS and RAM Mobile Data are two operators offering nationally networked RFDC support), and users rent air time for monthly fees. Terminals require special WAN radio modems, and data is transmitted via satellite networks with coverage in nearly all of North America.

Commercial RF Tag Companies

With over 50 companies listing their involvement in RF Tags, 37 vendors at SCAN-TECH USA '99 were supplying (or reported to be supplying) equipment.

AmaTech GmbH
Applied Wireless ID AWID
Balogh
Baltech Ag
Brady USA
Checkpoint Systems Inc.
Deister Electronic
Dynasys
E-code
Gemplus
HID I2R
id Systems Ltd
ID Tag Ltd.
Inside Technologies
Intermec Corporation
Metget AB
Microchip Technology Incorporated
Minec Sytems

Motorola Indala Corp
PAV Card
Philips Semiconductors
PinPoint Corporation
Poly-Flex Circuits
Polymer Flip Chip
RFID, INC.
Savi Technology
Sensormatic
Sihl
Single Chip Systems Corporation (SCS)
Sokymat SA
Sovereign Technologies Corporation
Symbol Technologies, Inc.
Tagmaster
Temic Semiconductors
Texas Instruments, Inc.
WhereNet (formerly WiData)
Zebra Technologies

Electronic Article Surveillance Systems

Often lumped with RFID are the Electronic Article Surveillance Systems which protects merchandise from theft. An EAS system has three components: 1) labels and hard tags—electronic sensors that are attached to merchandise; 2) deactivators and detachers—used at the point of sale to electronically deactivate labels and detach reusable hard tags as items are purchased; and 3) detectors that create a surveillance zone at exits or checkout aisles.

The EAS process begins by attaching labels or hard tags to merchandise. When an item is purchased, the label is deactivated or the hard tag is removed. However, if merchandise with an active label or hard tag is carried past the detector, an alarm sounds.

Over 800,000 EAS systems are installed worldwide, primarily in the retail market. This includes Apparel, Drug, Discount, Home Centers, Hypermarkets, Food, Entertainment, and Specialty stores.

EAS systems operate from a simple principle regardless of the manufacturer or the specific type of technology used: a transmitter sends a signal at defined frequencies to a receiver. This creates a surveillance area, usually at a checkout aisle or an exit in the case of retail stores. Upon entering the area, a tag or label with special characteristics creates a disturbance, which is detected by the receiver. The exact means by which the tag or label disrupts the signal is a distinctive part of different EAS systems. For example, tags or labels may alter the signal by using a simple semi-conductor junction (the basic building block of an integrated circuit), a tuned circuit composed of an inductor and capacitor, soft magnetic strips or wires, or vibrating resonators.

By design the disturbed signal created by the tag and detected by the receiver is distinctive and not likely to be created by natural circumstances. The tag is the key element, for it must create a unique signal to avoid false alarms. The disturbance in the electronic environment caused by a tag or label creates an alarm condition that usually indicate someone is shoplifting or removing a protected item from the area.

The nature of the technology dictates how wide the exit/entrance aisle may be. Systems are available that cover from a narrow aisle up to a wide mall store opening. Similarly, the type of technology affects the ease of shielding (blocking or de-tuning the signal), the visibility and size of the tag, the rate of false alarms, the percentage of detection rate (pick rate), and cost.

The physics of a particular EAS tag and resultant EAS technology determines which frequency range is used to create the surveillance area. EAS systems range from very low frequencies through the radio frequency range. Similarly, these different frequencies play a key role in establishing the features that affect operation.

Acousto-Magnetic

Acousto-magnetic EAS systems use a transmitter to create a surveillance area where tags and labels are detected. The transmitter sends a radio frequency signal at a frequency of 58 kHz (thousands of cycles per second), but the frequency is sent in pulses. The transmit signal energizes a tag in the surveillance zone. When the transmit signal pulse ends, the tag responds, emitting a single frequency signal like a tuning fork. The tag signal is at about the same frequency as the transmitter signal.

While the transmitter is off between pulses, the tag signal is detected by a receiver. A microcomputer checks the tag signal detected by the receiver to ensure it is at the right frequency, occurs in time synchronized to the transmitter, at the proper level, and at the correct repetition rate. If the criteria is met, an alarm occurs.

Electromagnetics

The electromagnetic EAS system creates a low frequency electromagnetic field (fundamental frequencies between 70 Hz and 1 kHz are typically used) between two pedestals at an exit or checkout aisle. The field continuously varies in strength and polarity, repeating a cycle from positive to negative and back to positive again. With each half cycle, the polarity of the magnetic field between the pedestals changes.

response to the changing magnetic field created by the transmitter, the magnetic field domain of the tag material abruptly "switches" as the field strength varies past a particular point, whether positive or negative, during each half of the transmit cycle. This abrupt change in the magnetic state of tag material generates a momentary signal that is rich in harmonics (multiples) of the fundamental frequency. Using electronic signal processing techniques, the system identifies that the harmonics are at the right frequencies and levels, and that they occur at the proper time in relation to the transmitter signal. If the criteria are met an alarm occurs.

Swept-RF

Like other EAS technologies, swept-rf uses a transmitter to create a surveillance area where tags and labels are detected. The transmitter sends a signal that varies between 7.4 and 8.8 MHz (millions of cycles per second), which is why it is called swept; it sweeps over a range of frequencies.

The transmitter signal energizes the swept-rf tag or label, which is composed of a circuit containing a capacitor and an inductor or coil, both of which store electrical energy. When connected together in a loop, the components can pass energy back and forth or "resonate." The

frequency at which the circuit resonates is controlled by matching the storage capacity of the coil and capacitor. The tag responds by emitting a signal that is detected by a receiver.

In addition to the small tag signal, the receiver also responds to the much larger transmitter signal. By detecting a phase difference between these two signals, and other properties of the tag signal, the receiver recognizes the presence of a tag and generates an alarm.

Microwave Technology

The system is composed of a transmitter, a synchronous receiver, a microprocessor-controlled detector, and an alarm. The transmitter produces two signals to excite the tag. One is a high frequency carrier signal and the other is a much lower frequency electrostatic signal. In North America the high frequency signal is hopped over a band of 902-906 MHz in distinct groups of 50 frequencies to avoid interference from adjacent systems. In Europe the high frequency is between 2402 and 2486 MHz and is not hopped; each system has its own unique frequency assigned.

The lower frequency is modulation signal is 111.5 kHz. It is a non propagating electrostatic signal that limits the range of the high frequency RF field to the desired surveillance zone. This prevents the signals from traveling large distances and interfering with other systems or causing alarms due to tags on articles just outside the surveillance zone.

The tag is composed of a microwave diode and a combination antenna for the receipt of the high and low frequency. When introduced into the field of the transmitter, the tag combines or mixes the two fields and re-radiates the combined signal to the high frequency receiver. The resultant 111.5 kHz modulation of the high frequency signal is amplified and compared to a reference in the detector to ensure it is at the correct frequency and level. If correct, an alarm is initiated.

Additional PNNL References

http://www.pnl.gov/greenie/3_7_97/mini.htm
http://electronics.pnl.gov:2080/tag_3.pdf