



PDHengineer.com

Course N^o E-1008

RFID Fundamentals



To receive credit for this course

This document is the course text. You may review this material at your leisure either before or after you purchase the course. To purchase this course, click on the course overview page:

<http://www.pdengineer.com/pages/E-1008.htm>

or type the link into your browser. Next, click on the **Take Quiz** button at the bottom of the course overview page. If you already have an account, log in to purchase the course. If you do not have a PDHengineer.com account, click the **New User Sign Up** link to create your account.



After logging in and purchasing the course, you can take the online quiz immediately or you can wait until another day if you have not yet reviewed the course text. When you complete the online quiz, your score will automatically be calculated. If you receive a passing score, you may instantly download your certificate of completion. If you do not pass on your first try, you can retake the quiz as many times as needed by simply logging into your PDHengineer.com account and clicking on the link **Courses Purchased But Not Completed**.

If you have any questions, please call us toll-free at 877 500-7145.



PDHengineer.com
5870 Highway 6 North, Suite 310
Houston, TX 77084
Toll Free: 877 500-7145
administrator@PDHengineer.com



RFID Fundamentals

Online Course No. E-1008

Credits: 1 PDH

Introduction

The ancient truism of generals, that armies advance only as far as their lines of supply can reach, holds a seed of truth for all public or private sector endeavors: Unless you have good logistical control over product pipelines, you will likely come up short when you attempt to expand your market share. For example, effective public service logistics (clean water, electricity, roads, etc.) are an economic keystone of all modern industrialized nations; without them modern economies would fall into chaos. They are a major force in determining zoning and development regulations, since uncontrolled growth in one focused area would put a terrible strain on the overall infrastructure. In the same way, manufacturing/retail concerns require their own logistical controls to survive (and hopefully be profitable). An important element of this is the control of information about materials: how much product is in stock? how much is in process? how much raw material is available? and, most importantly, where *is* it all?

Traditionally, this has been achieved through paper – lots and lots of paper. Incoming, outgoing, in-transit, in-process, in-storage and countless other designations custom suited to the product/process being tracked, all having their status recorded and updated on paper, often multiple copies, all requiring untold hours to maintain. The last 40 years have seen computers revolutionize the record-keeping end of this equation, with data about products in the pipeline stored electronically for easy access through automated database searches. This change has increased logistical efficiency tremendously, but a bottleneck at the head end of the system still plagues many; how do you get the information into the system in the first place? Around the world, many people still spend thousands of hours every year doing data entry, moving information from one piece of paper containing information printed from a supplier's computer system into their own organizations computer system. With the obvious limitations of this approach, many installations embraced barcodes or other visually machine readable symbologies to carry identification numbers that can be used to query their own or a vendor's database for more information about the product/material that the machine readable number was assigned to. They are easy to produce using standard laser or thermal printers, with many symbol sets in the public domain and non-proprietary, so installations can be very low cost (other than the readers themselves, and even those prices continue to fall as technology advances). Machine readable printed labels do have drawbacks, however: they can become damaged in shipping or plant floor accidents to the extent where they are no longer readable by the scanner, and in the end a printed label is only as good as the printer that generates it. Also, most public domain barcodes are not suited to storing any more than a few dozen characters of data, making them well suited for providing database reference numbers but not so useful when portable, data-rich onboard machine readable information is desired. A solution to these problems that is gaining acceptance is RFID technology, a wireless communications approach that has many of the advantages of printed barcodes and other symbols but eliminates some of the drawbacks.

RFID (Radio Frequency Identification) systems, when even noticed by the general public at all, are most commonly associated with retail anti-theft security, non-contact key cards, or some automobiles that require "key proximity" as an added security measure for the ignition switch. That RFID would be integrated into these uses is not surprising, as the generally small size of the RFID modules themselves make them an ideal choice for integration with key cards, labels on merchandise, or any other item that would otherwise require human/machine vision or physical contact to identify. However, RFID can be used for more than just a wireless security measure – the technology is increasingly used in warehousing, shipping, manufacturing and a continually growing list of other purposes all over the world to provide physically robust and potentially secure point-of-use identification, tracking, and asset management data for whatever the RFID tags are assigned to.

History:

Like many technologies, RFID can trace its roots to the necessities of war. Radar made major advances during WWII, aiding all sides in the conflict with their search for enemy surface ships and airplanes electronically. However a blip on a screen does not tell the operator who is friend or foe, and both the British and Americans developed "call-reply" transponder type systems that would provide ground stations with some identification of friendly aircraft (assuming the pilot remembered to turn it on!). When in range of the radar station, the IFF (Identify Friend or Foe) system was triggered to signal back that the aircraft was friendly by sending a predetermined code, much like modern day RFID. Modern descendants of these IFF transponders are standard issue in military aircraft, as well as commercial jets and many private aircraft to aid in air traffic control and collision avoidance.

Development continued, and with the birth of the semi-conductor electronics age RFID tags and the associated reader/interrogators became more feasible. Starting with EAS (Electronic Article Surveillance) used for asset management in retail establishments and libraries the small attached or integrated tags became ubiquitous in the modern marketplace. In its most basic form, anti-theft one bit tags are simply a small antenna that resonates when in the field generated at the interrogator gate, usually at the exit of the establishment. The interrogator looks for a change in load of a profile indicative of the tag in question on its transmission antenna, and triggers an alarm if found. Depending on the variety of system, the tag is either removed from the item or deactivated at checkout (usually by placing the item in a strong magnetic field, changing the physical electromagnetic responsiveness of the tag) to allow egress without triggering the security alarm.

With the introduction of the integrated circuit in the 1960's, data rich RFIDs time had finally arrived. The early 1970's saw the first integrated read-write RFID tags, and the first patents for door security using RFID. The USDA funded research that led to the development of passive RFID ear tags for cattle so that identification of individual animals could be automated. Today, use of such tags are not only commonplace, they are quickly becoming a requirement around the world as governmental regulatory agencies attempt to protect the food supply against "mad cow" disease and other livestock pathogens. Communicating on a 125KHz carrier frequency, these tags were (and still are) well suited for short range, low data content signals (e.g. an animals identification number).

It was soon recognized that longer read distances and higher data rates would be needed for many other potential applications, so 13.56MHz systems were developed in the 1980s. Initially used for pallet tracking and other large item tagging, 13.56 MHz systems are now also used for building security and "swipeless" credit or debit cards. Longer read distances make it easier to use, and faster data rates allow for greater encryption of the entry codes without annoying delays. Further developments were made in the 1990's, upping the carrier frequencies even higher into the UHF range (300MHz to 3 GHz) but RFID tags of this type generally operate between 866 MHz to 960 MHz. It is these varieties that are currently the focus of the EPC (Electronic Product Code) standardization effort, a global enterprise that will hopefully allow any product around the world to be identified through a serial number held in the tag and a database available over the internet.

Technological Overview:

Several varieties of wireless systems can rightly be called RFID, from the original single bit security systems based on inductive resonance to magneto-acoustic systems that rely on magnetostriction derived vibration to alert interrogators to their presence. However, these systems do not provide much by way of data, other than tag presence, since they react to the interrogator field as electro-magnetic and electro-

mechanical devices and are not capable of semi-intelligent data storage. Going forward, RFID's true value is in providing multi-item differentiation and identification, and for this integrated circuit based devices are required.

In general, RFID systems of this type consist of at least two parts: the data storage device; and the reader, called the interrogator. The storage device itself, the "tag", consists of an antenna, modulating circuitry, and non-volatile memory containing relevant information that is transmitted by the modulation circuitry when the tag is queried by an interrogator reading device. The amount of information can range from just a single bit up to several megabytes. An interrogator consists of an antenna, RF transmission and demodulation electronics, and usually provides the demodulated data contained on the tag to a supervisory system, like an inventory control network, machine fabrication line controllers, or building entry security system.

RFID tags are queried for stored data by the interrogator using a RF electromagnetic carrier wave. Two main designations exist for RFID – passive and active. A hybrid of these two approaches is called “semi-passive”, using some of the elements of both active and passive systems (e.g. a tag that is "passive" for standard reading incidents, but is "active" when data on it is updated wirelessly). Tags in active systems carry an onboard energy source for powering the transmission of data and general communication with the interrogator. Passive tag systems use the RF wave transmitted by the interrogator to power its systems and communicate with the interrogator, using an approach called backscatter modulation.

ACTIVE RFID:

Active systems use the higher end of the RFID frequency spectrum, and are most often used when large amounts of data are to be stored on the tag, or fairly long communication distances are required by the application such as semi-trailer trucking depots. The transmission distances and robustness of active systems are dependent on the power output of the active transmitting tag/interrogator pair. In applications where higher communications speeds, large volumes of data or long transmission distances are needed, active transmission tags are better suited. Active tags operate along the same lines as all standard RF data transmission.

PASSIVE RFID:

Passive systems use either propagation coupling or inductive coupling, depending on the frequency range of the tag. In the case of inductive coupling (used with lower frequency tags, up to ≈ 15 MHz) the antennas for the interrogator and tag together can be thought of as being analogous to an air core transformer, with the interrogator antenna being the primary coil and tag antenna the secondary. The interrogator produces a carrier signal that, by Ampere's and Faraday's laws, induces a current on the closed conductive circuit of the tag antenna. This induced current is proportional to three factors: strength of the broadcast EM field from the interrogator; distance between the transmitting and tag antennas; and orientation of the tag antenna in the generated field. Additionally, if the tag antenna length is a multiple of the wavelength of the transmitted carrier wave or is tuned with resonant components (inductors and capacitors), greater resonant coupling is achieved, improving the communications link.

Lower frequency passive systems have read distances of a few centimeters (125 KHz) up to 3 meters (866 MHz to 960 MHz). The quality of inductively coupled passive modulation systems is more dependent on the quality of electromagnetic coupling between the interrogator and tag antenna than the power output of the interrogator.

In the case of propagation coupling, used with UHF and higher frequency systems, the interrogator "shoots" a high frequency carrier wave (in the microwave range) to the tag antenna. The length of this antenna, a standard dipole or similar antenna configuration, is selected based on the wavelength of the carrier wave (e.g. 2.45GHz = 12.23 cm). The amount of energy collected by the antenna is sufficient, with modern low power semi-conductor technology, to power the tag's transmission circuitry (just like with inductively coupled systems, but at much lower power) but without resonant components. Since the higher frequencies (and thus shorter wavelengths) are of the same physical scale as conveniently sized dipole antennas, tuning components are unnecessary to achieve resonance. Microwave/high frequency propagation coupled systems are more complicated than their low frequency brethren, and are thus more expensive - because of the low energy conveyed by the coupling, microwave RFID systems generally are semi-passive in nature. The majority of new installations of RFID systems are of a low frequency variety, so for this introduction to RFID we have focused our discussions on inductively coupled systems.

Passive systems are valued in RFID designs over their active cousins in many applications because of their intrinsic bandwidth efficiency, low power consumption and tag segregation ability – the only devices transmitting are those within close range of the interrogator, reducing the chance of mistaken identification. In passive or semi-passive RFID applications, current induced by the interrogator on the tag antenna is rectified and used as the power source for the RFID data retrieval and modulation circuitry. This allows smaller and less obtrusive units to be produced because the additional mass required by a power source is absent from the tag body. In situations where both writing and reading from the tag are required, but the benefits of backscatter modulation is desired, hybrid semi-passive tags can be used in conjunction with an internal/external power source in addition to the interrogator to write to their onboard PROM (Programmable Read Only Memory, erasable or otherwise).

In applications where indeterminately long term, stable storage of data is needed, passive systems can have an advantage over active systems since the device does not require a local power source for storage or transmission activities, and thus can be stored nearly indefinitely without tag maintenance or loss of data.

SEMI-PASSIVE RFID:

While they often use the same sort of backscatter communication channel as passive systems do, semi-passive RFID systems generally have much more complex circuitry in the tags to handle the extra data memory and often have the ability to be updated remotely by an interrogator. Due to these higher power needs, they require an onboard power source like fully active RFID systems.

PASSIVE BACKSCATTER RFID:

Backscatter RFID systems are quite a bit different from standard RF transmission. As previously described for inductively coupled systems, the interrogator generates a RF carrier wave that induces current on the tuned tag antenna when the tag is within range of the field. Once the induced voltage on the tag antenna reaches a sufficient power level to power the unit and trigger transmission, modulation circuitry sequentially clocks out the data stream. Generally speaking, in digital RF transmission modulation can occur in at least one of three ways: Amplitude Shift Keying (ASK); Phase Shift Keying (PSK); and Frequency Shift Keying (FSK). PSK and FSK are not commonly used in passive systems, since they would require significantly more complex circuitry and hardware than an ASK system. ASK is achieved by simply shorting a section of the antenna tuning circuit in a pattern corresponding to its stored data. Since changing the inductive or capacitive values of a tuned antenna circuit will alter its resonant frequency, and electrically shorting a section of the antenna will cause changes to circuit reactance, the amount of energy induced on the antenna circuit is changed. At the interrogator, a small fluctuation in the voltage applied to the transmission antenna occurs since the magnetically coupled circuit (interrogator and

tag) experiences a changing load as the tag antenna goes from resonant to non-resonant. The interrogator continuously monitors fluctuations in this output voltage, demodulating any patterns that emerge. This reproduces the data transmitted from the RFID device. Since this variation can be very small in comparison to the voltage level, the practical output power of the interrogator is limited by the sensitivity of the demodulating circuit to this tiny fluctuation. Thus, increasing the read range of a backscatter RFID system is not just a simple matter of increasing the transmission power, like what would be possible with an active RFID system, but instead requires greater care in the design and construction of the tag so as to optimize the magnetic coupling between it and the interrogator.

MODULATION TECHNIQUES:

Several encoding protocols exist for both passive and active systems, most being proprietary to the manufacturer of the RFID tag and interrogator system. For example, Biphase-L encoding, also called Manchester encoding, is used for the transmission of data in several RFID products from Microchip Technologies¹. In their 13.56 MHz MCRFxxx passive RFID product lines, the monolithic integrated circuit in the tag has an internal oscillation circuit that generates a 70KHz timing signal used to sequentially clock out the data stored in the onboard memory array using ASK. Manchester encoding combines both the transmitted data and bit frame timing by having each symbol contain a low/high (bit = 0) or high/low (bit = 1) transition. In this way, the demodulating device can synchronize bit frames with the tag. A representation of a sample Manchester encoding bitstream is shown in Figure 1.

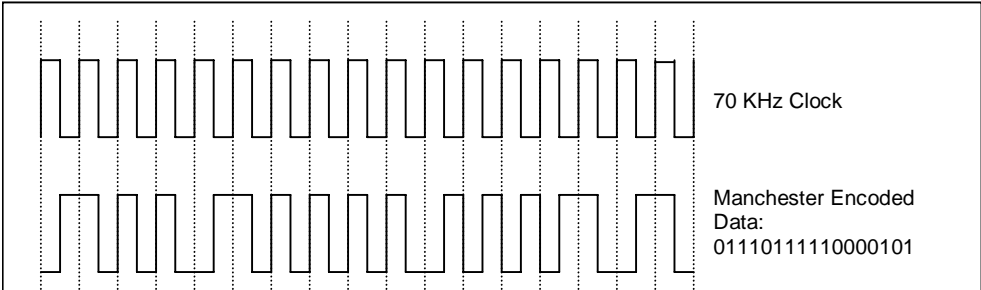


Figure 1: Example Manchester encoding sequence. The polarity of the transitions in the Manchester encoded data bitstream on the negative slope of the transmission clock signal determine the value of the binary datum that is transmitted, with high to low being logic 0 and low to high being logic 1.

The above example is only for one manufacturer with one specific RFID implementation, but provides a glimpse of some of the nuts-and-bolts, "level 1" protocols that underlie all RFID applications.

STANDARDS:

Different manufacturers and vendors have different approaches to solve the same identification problems, which is to be expected in a relatively young industry without well-established standards. However, basic standards have come into being as needed during the development of the technology, and continue today.

ISO (International Standards Agency) was first to lay standards for spectrum usage and power output, in conjunction with various governmental agencies around the world (e.g. the FCC in the USA). Limited

¹ Microchip Technologies Inc., Chandler, AZ 85224 USA

to technical standards for frequency, range, power and the like, the door was wide open for usage protocols to develop on a case by case and vendor by vendor basis.

Worldwide frequency allocations for radio frequency identification

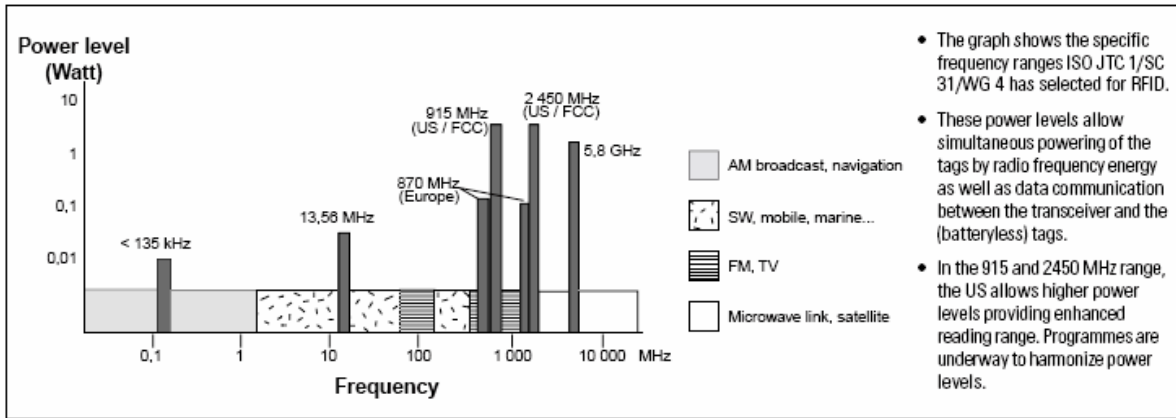


Figure 2: Chart originally published in *Information technology - Radio frequency identification (RFID) and the world of radio regulations*, Josef Schuermann, ISO Bulletin May 2000, p4.

EPC Global, a non-profit institution based on the work of the Auto-ID center at the Massachusetts Institute of Technology (MIT), was formed to manage and support the EPC (Electronic Product Code) global architecture developed by academic research there. Much like the familiar UPC barcode markings on many retail products, EPC codes contain identification codes for the products they are assigned to. However, since EPC are stored on RFID tags and not barcodes, they have the capacity for much richer data set to be carried onboard. This allows for EPC to be used up and down the supply chain: the same code architecture and devices used for identifying the contents of shipping containers and pallets can also be used for individually identifying the singular products shipped by those means. By registering codes with EPC Global, any product or container tagged using their standards will be able to be identified anywhere in the world by checking the EPC database, from whole pallets down to single widgets. Adoption of EPC will not only allow for greater efficiency in retail checkout (instead of individually scanning each item's UPC code, purchased items need only be within reading range of the interrogator) but the greater data capacity will allow for traceability of individual items throughout the supply chain. With access to the EPC database you could scan a can of soup sitting on a grocery shelf and know not only the type of product, but when it was made, what plant it was manufactured in, and maybe (in the future) even the ingredients and nutritional information. Essentially, it can contain whatever the manufacturer chooses to write on the tag, as long as it follows the EPC standards. In the same way that UPC barcodes took a few years to gain in acceptance, EPC tags will most likely take the same course. If history is any guide, given time, RFID EPC tags will become just as ubiquitous.

Conclusion

Since early 2005 the US Dept. of Defense has required that suppliers include a data-rich RFID identification tag to facilitate inventory logistics when their products are delivered containerized or palletized. US retailing giant Wal-Mart followed suit by mandating their 100 top vendors to supply RFID tags with palletized shipments, with all other vendors required to do the same by late 2006. Because of the immense size of these organizations, the effects of these policies will ripple outward and strongly impact shipping and warehousing methods around the world, and the standardization efforts underway with EPC infrastructure will help streamline this effect.

The expanding use of RFID isn't just limited to shipping and warehousing logistics. Many manufacturing facilities use RFID modules as mobile databases for palletized assembly lines, using them to carry manufacturing data as the "widget-in-process" works its way through the plant. Environmentally robust and biologically inert RFID tags have been put to use for ear tagging or subcutaneous implantation, used in the dairy and cattle industry for many years to track individual animals in the herd for improved production data. In the same vein, tags about the size of a grain of rice can be inserted under the skin of dogs and cats, so lost animals can be returned to their owners. Some are even evaluating programs for similar implants to be used in finding and identifying missing children, with parents having their children implanted with RFID tags in the event standard identification techniques are impossible. In some nations, plans are being made to require the implanting of RFID tags in passports and other travel documents to speed travel through customs. The technology is not so far away that RFID tags could be made small enough for integration within individual threads in cloth for the apparel industry, potentially used for retail security and/or EPC codes. With the tag in place, it could also be used for controlling personalized automatic environmental controls for the wearer of the garment, keyless entry, or anything else that could be automated if a system had some means of both identifying the presence of a person and who they were. Much like in the internet browser world, we could someday have thousands of "personal cookies" spread across any establishments we would frequent that could automatically provide any number of personalized services (or annoyances) whenever a tag wearer came into range of an RFID interrogator.

Not unreasonably, many personal privacy advocates believe the intrinsically hidden, silent nature of the devices are too tempting a method for abuse by both governmental and commercial interests to track the movements and habits of individuals, for either benign or nefarious purposes. With continuing advances in electronic micro-miniaturization and new and novel RFID fabrication techniques, RFID technology promises to increasingly become more ubiquitous, for good or for ill.

References:

<http://www.epcglobalinc.org/about/faqs.html>
<http://www.epcglobalinc.org/about/about.html>
http://www.rfidnews.com/iso_11784.html
<http://jproc.ca/sari/sariff.html>
<http://www.rfidjournal.com/article/articleview/1338/2/129/>
<http://www.rfidjournal.com/faq/16/48>
<http://www.rfid-handbook.de/rfid/frequencies.html>
http://www.rfid-handbook.de/downloads/E2E_chapter03-rfid-handbook.pdf
<http://www.aimglobal.org/standards/rfidstds/RFIDStandard.asp>
http://epsfiles.intermec.com/eps_files/eps_articles/TrendsStandardBehavior_article_web.pdf
<http://www.iso.org/iso/en/commcentre/pdf/Radio0005.pdf>
<http://ww1.microchip.com/downloads/en/devicedoc/21299e.pdf>