RFID Fundamentals

An Online Continuing Education Course for Engineers

Course Number: E-1008

Credit: 1 Hour / 1 PDH / 1 CPD

RFID Fundamentals

Erich C. Hoffacker, P.E.

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 several decades 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 at 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 on-board machine readable information is desired. A solution to many of these issues can be found in RFID technology, a wireless communications approach that has many of the advantages of printed barcodes and other symbols but eliminates many of the drawbacks. And, like many young technologies, developers are continuously finding new applications beyond its original purpose.

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 or credit cards, or many automobiles that require "key proximity" as an added security measure for ignition. 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 widely 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 and vehicles, 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 common in the modern marketplace. In its most basic form, anti-theft one bit tags are simply a small antenna that resonates when within the EM 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 animal's identification number).

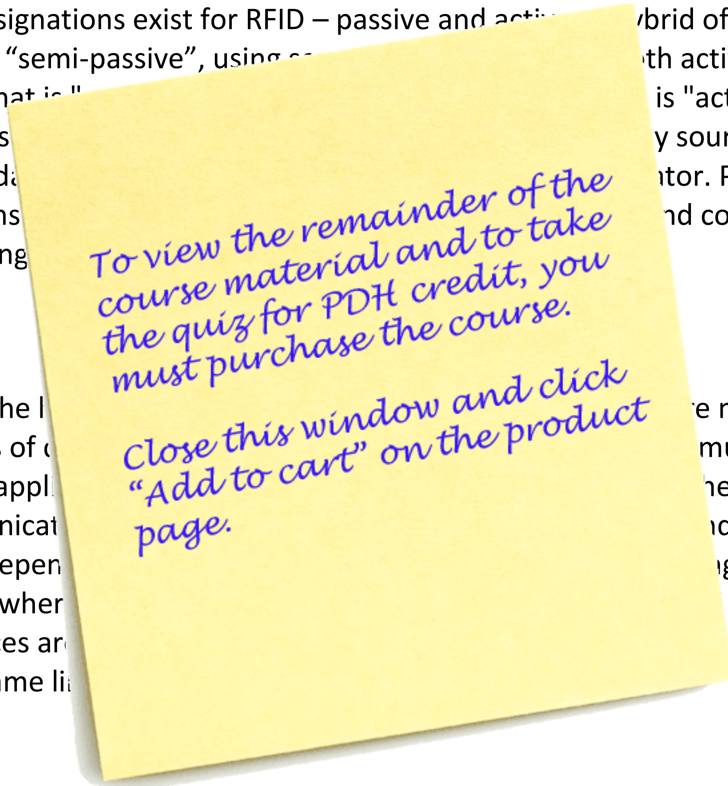
It was soon recognized that the potential for longer read distances and higher data rates would be needed for many other applications, so in an attempt to meet that need 13.56MHz systems were developed in the 1980s. Initially (and still) used for pallet tracking and other large item tagging, 13.56 MHz systems are now also used for building security, "swipeless" credit or debit cards and NFC (Near Field Communications) enabled mobile devices. Faster data rates allow for greater encryption of data without annoying delays, and this speed also provides sufficient bandwidth for multiple data devices to communicate (from a human perspective) almost simultaneously. 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. Both the 13.56MHz and the UHF varieties are utilized in 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 meaningful 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. NFC enabled devices (e.g. smartphones) differ from this architecture somewhat in that, being programmable devices themselves, they can be either the interrogator or tag depending on the application as well as being able to use that same band (albeit with a different data protocol) to connect to other NFC enabled devices.

RFID tags are queried for stored data by the interrogator using a RF electromagnetic carrier
wave. Two main designations exist for RFID – passive and acti ybrid of these two
approaches is called "semi-passive", using s th active and passive
systems (e.g. a tag that i is "active" when data on
it is updated wireless y source for powering
the transmission of da tor. Passive tag systems
use the RF wave trans nd communicate with
the interrogator, using



ACTIVE RFID:

Active systems use the l e most often used
when large amounts of munication distances
are required by the appl he case of intelligent
NFC devices communicat nd robustness of
active systems are depen g tag/interrogator
pair. In applications wher data or long
transmission distances ar . Active tags
operate along the same li

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 ≈15MHz) 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 (125KHz) 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.