how it works

FIND OUT HOW RETAILERS FIGHT SHOPLIFTING WITH ELECTRONIC SENTRIES THAT AUTOMATICALLY SCAN YOUR BAGS AND POCKETS FOR STOLEN ITEMS EACH TIME YOU EXIT THEIR STORES.

Stop! Thief!

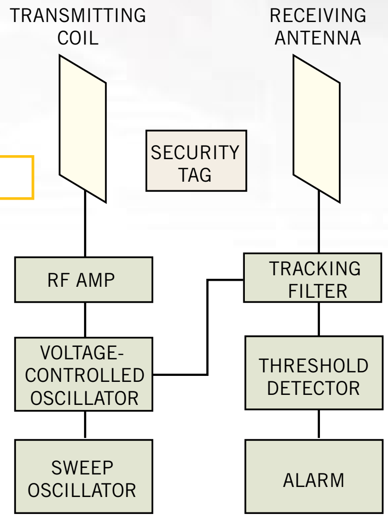
By Warren Webb, Technical Editor

WE HAVE ALL BEEN ANNOYED by the false alarms and bulky tags of EAS (electronic-article-surveillance) systems that are now on guard in most retail stores. Along with closed-circuit television, EAS is part of retailers' high-tech war on shoplifting that costs the industry an estimated $10 billion per year. Losses are so high that retailers easily justify the high-priced electronic systems to deter theft. EAS systems are characterized by large antenna panels at store exits and security tags of all sizes attached to high-risk goods.

EAS technical performance and retail use have steadily increased since the introduction of the first crude systems in the 1960s. EAS manufacturers have enjoyed rising sales, because the installation of a system at one retailer drives all the shoplifters to another shop, which in turn justifies the sale of another system. Even with its long history, no industry-wide EAS standards exist, and most EAS technologies and techniques are proprietary.

The basic principle behind all EAS systems includes a transmitter to create an electromagnetic field across the store's exit area and a receiver that can detect variations in the field. Small tuned circuits or magnetic material inside security tags that pass through the exit modify the field enough for the receiver to detect the change and activate an alarm. The retailer attaches the tags to high-risk items, and the EAS system notifies him or her when a tag passes through the exit field. You must remove or deactivate security tags when the item is sold to prevent the alarm from sounding.

Figure 1



RF EAS systems constantly sweep through a narrow frequency spectrum to detect the presence of security tags in the exit field.

Although all EAS systems look similar, several types are in use today, each with advantages and disadvantages. RF and acoustomagnetic systems are the most sophisticated and supply more than half of the EAS market. Early microwave systems, which provide marginal security, are no longer manufactured, yet they still account for approximately 20% of current systems. Electromagnetic systems, very popular with European retailers, have less than 15% of the US market. EAS users select between the available types depending on system cost, detection rates, distance between exit gates, tag size, merchandise type, and cost of consumables. Unfortunately, the various systems are not compatible with each other, so retailers have to commit to one type and face complete equipment replacement if technology, detection rates, or merchandise changes lead them to another type.

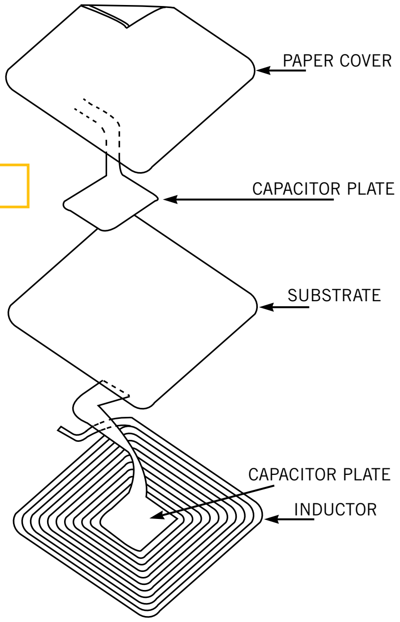
FIELD FLUCTUATIONS

Swept-RF technology dominates the most popular EAS systems. A typical RF system consists of transmitter and receiver panels spaced as far as 80 in. apart (**Figure 1**). The rectangular or oval panels are antennas containing multiple turns of wire wound in circular and figure-eight patterns to maximize both vertical and horizontal electromagnetic fields. The frequency of operation varies by manufacturer; however, most operate in the 1- to 10-MHz range. Many vendors have settled on 8.2 MHz, because the higher frequency results in smaller inductive and capacitive components. The transmitter sweeps approximately ±15% of the nominal center frequency to allow for small variations in the security tag's resonant frequency. If a tag is present in the field when the transmitter sweeps through its resonant frequency, the tuned circuit absorbs some of the field energy, and the receiver signal strength changes.

Early security tags were made from hard plastic and attached to the item with a pin and a locking mechanism. Each tag contains a resonant circuit tuned to the operating frequency of the EAS system. The retailer must remove the tags with a special detacher when a customer purchases the item. These reusable, hard plastic tags are still popular for soft, nonconducting goods, such as clothing, and retailers can purchase them for as little as 30 cents each.

Disposable RF tags are formed by depositing conductive traces on both sides of an insulating substrate similar to flexible pc boards (**Figure 2**). The substrate is thin enough to form the dielectric material for printed capacitors. The substrate and conductive layers are typically sandwiched between paper layers to protect and hide the tag. These features allow designers to create an LC tank circuit with any desired resonant frequency. Dimples created in the manufacturing process provide connections between layers or fusible links that you can use to detune and, therefore, deactivate the circuit. These disposable tags cost less than five cents each, and you can easily camouflage them with a simulated bar code or advertising message printed on the top surface.

Figure 2



To protect high-risk merchandise, retailers attach a paper-thin, LC tank circuit tuned to the EAS operating frequency.

Figure A

EAS systems monitor tiny electromagnetic-field changes to protect retailers from shoplifters (courtesy Sensormatic Electronics Corp, www.sensormatic.com).

If the security tag is disposable, and therefore leaves the store, the merchant must provide a deactivator at the point of purchase. If a security tag remains active and a consumer brings it into another store in a bag, it could cause confusion. The deactivator produces an electric field with sufficient amplitude to blow the tag's built-in fusible link. Vendors now provide deactivators that are assembled into bar-code scanners to prevent dishonest employees from deactivating an item without recording the payment.

Newer acoustomagnetic systems are rapidly becoming the preferred EAS technology for retailers that sell metal objects or use metal shopping carts. Acoustomagnetic systems employ a special material in the security tags that deforms in the presence of a magnetic field. When tuned with a magnetic bias strip, the magnetostrictive material mechanically vibrates as it passes through the exit field. The receiver looks for ringing at the resonant frequency to detect security tags. A deactivator demagnetizes the bias strip so that ringing occurs outside of the receiver's range.

Acoustomagnetic systems cost about twice as much as comparable RF systems, but they are quite robust, even detecting security tags inside foil-lined bags. One disadvantage of these systems is that some magnetic deactivators are strong enough to accidentally erase or modify the magnetic strip on credit cards.

TAG, YOU'RE IT!

Some retailers now require manufacturers to include security tags inside merchandise packaging. This technique, called source tagging, saves retailers the labor cost associated with applying the tags. Some manufacturers have proposed integrating security tags into the product. For example, RF tags sewn into garments as a brand label would be difficult to remove. Currently, source tagging is not universal because some retailers do not have EAS systems and have no means to deactivate the tags.

You can reach Technical Editor Warren Webb at 1-858-513-3713, fax 1-858-486-3646, e-mail wwwebb@cts.com.

There is always a safety concern when designers create intentional electromagnetic fields. The FDA has issued a safety notice to neurologists and emergency-room physicians stating that EAS systems, along with airport metal detectors, have been the subject of studies to determine their effect on medical implants, such as pacemakers, defibrillators, and spinal-cord stimulators. Although the number of reported complaints has been very small, this possible interaction will affect the design of both EAS systems and implantable medical devices (**Reference 1**).

You can describe most of today's EAS systems as 1-bit subsets of RFID technology. Retailers of the future will probably use manufacturer-supplied RFID tags to combine EAS functions, customer checkout, and inventory tracking. Each tag will deliver a unique code upon interrogation, and deactivation will be unnecessary because the EAS system will have a record of purchases. In fact, with a common Internet database, EAS systems will be able to identify stolen goods from any retailer.□

Reference

1. Casamento, Jon P, "Characterizing electromagnetic fields of common electronic article surveillance systems," *Compliance Engineering*, September 1999.