

READING BETWEEN

SECURITY AND SUPPLY-CHAIN-MANAGEMENT CONCERNS ARE AMPLIFYING THE RFID HYPE. CONFLICTING STANDARDS, PRIVACY CONCERNS, AND THE THREAT OF LEGISLATIVE OVERSIGHT, THOUGH, THREATEN TO MUTE THE VOLUME. LISTEN IN.

THREE DECADES ago, a 10-pack of Juicy Fruit gum and a cashier at a Marsh supermarket in Troy, OH, were the participants in the first successful test of what we now know as the

UPC (universal product code) bar-code system. Evolution of the bar-code system continues; for example, US and European standards-group representatives recently agreed on a common 14-digit format that, beginning in January 2005, bar-code readers worldwide must support. But, all in all, bar codes today are mature, pervasive, and well-understood. (Some ex-presidents may beg to differ on that last point, though. Remember George HW Bush's befuddlement when, on the 1992 primary-campaign trail in New Hampshire, he unsuccessfully attempted to use a

bar-code scanner in a grocery store?)

Technology marches on, though, and an up-and-coming contender to the product-identification throne has emerged: the RFID (radio-frequency-identification) device. Ironically, RFID technology is almost as old as bar codes, which in 1934 received their first patents. Great Britain's Royal Air Force employed RFID-like techniques to distinguish between friendly and enemy incoming airplanes during World War II, and Harry Stockman's October 1948 treatise, "Communication by Means of Reflected Power" in *The Proceedings of the IRE* (Institute of Radio Engineers) first detailed the theory and implementation of RFID. Prolific inventor Charles Walton in 1973 received the first RFID patent for a passive RFID-based door-lock reader. Walton coincidentally shares the same last name as the late Sam Walton, the founder of Wal-Mart, which, along with the US Department of Defense, has played a leading role in spurring current RFID deployments.

If RFID is such a timeworn

technology, why then has the interest in it accelerated so dramatically in the past few years? Part of the reason is chip capability; thanks to Moore's Law, passive RFIDs sell for less than 50 cents in high volumes, and analysts predict they'll sell for less than five cents in high volumes by the end of this decade. Adequate infrastructure capability is also important; the dot.com explosion of the late 1990s fueled the development of networking equipment and powerful servers with speedy CPUs and I/O connectivity and containing ample memory and hard drives, and the subsequent dot.com implosion has resulted in copious underused network bandwidth begging for someone to harness it.

The final piece of the interest-in-RFID puzzle comes from customers' needs. Manufacturers, distributors, and retailers all want to as much as possible automate their sys-

tems to eliminate expensive and unreliable human beings from the process, and they aspire to have timely and accurate insight into the location of individual products at a given time and into various product-staging locations' inventories. If possible, they'd like to extend their insight beyond the store, to link each product with an individual consumer, and, in combination with other collected data, to ascertain

the means by which they can lure that consumer into buying even more (see sidebar "Privacy concerns"). Governments, too, have an interest in learning as much as is legally possible about what their countries' citizens and residents are up to.

As is the case with nearly every budding application in its infancy or adolescence, a diversity of incompatible options has emerged to address the various challenges that invariably arise (**Reference 1**). With RFID, these differences begin with the fundamental means by which the RFID tag communicates with its reader. A passive RFID tag contains no power source of its own.

<i>At a glance</i>	50
<i>Privacy concerns</i>	52
<i>Application teasers</i>	54
<i>For more information</i>	58

THE LIN ES


RFIDs confront the venerable bar code



Instead, the reader powers, or “harvests,” power using either inductive coupling or electromagnetic capture in a process in which the reader “excites” the RFID tag. An *active* RFID tag, conversely, includes a battery, substantially increasing its cost but also potentially enhancing its functional capabilities, along with its operating range. A *semipassive* tag, an intermediary approach, runs the chip’s standby circuitry from a battery but draws power from the reader during active communication sessions.

RFID readers and tags also broadcast and receive using a diversity of frequency ranges. Low-frequency RFID systems operate at 125 to 134 kHz, for US and international use, respectively, and 13.56 MHz, another international standard, is the most common high frequency. UHF (ultra-high-frequency) RFID systems range from 866 to 960 MHz, and microwave systems operate at 2.4 to 5.8 GHz. With all other factors being equal, high-frequency RFIDs have longer range than their low-frequency counterparts, fundamentally because near-field effects don’t degrade high-frequency RFIDs’ signals. If a tag is less than one wavelength away from a reader, the signal decays with the cube of the distance; beyond one wavelength, the signal decays with the square of the distance. High-frequency RFIDs can also more quickly transmit and receive data.

Conversely, high-frequency tags and readers are more expensive and burn more power than their low-frequency peers, and environmental factors, such as packaging, moisture, and nearby metallic items, adversely attenuate high-frequency devices’ signals more than their low-frequency counterparts. You also



AT A GLANCE

- ▷ Everything old is new again: RFID is many decades old in concept, but implementations have rapidly ramped in recent years.
- ▷ Frequencies, modulation schemes, power techniques, and other incompatibilities hinder widespread adoption but will eventually settle out.
- ▷ The amount of storage memory on-board the RFID tag depends in part on whether your RFID reader is connected to the Internet, an intranet, or both.
- ▷ Opportunities for vendors selling hardware and software that stores, transfers, and transforms RFID data may far exceed the RFID-tag market-growth potential.
- ▷ Ensuring that the RFID revolution blossoms without trampling individuals’ privacy rights will require consumer awareness, legislative oversight and private-sector restraint.

need to be aware, when specifying and designing RFID gear, that a frequency freely usable in some parts of the world may not apply in others or may require an expensive and time-consuming licensing process. Unlicensed frequency bands are also subject to spectrum corruption, a factor that anyone who has tried to simultaneously operate a microwave oven, a cordless phone, a Wi-Fi access point and client, and a Bluetooth-paired set of equipment has experienced (Reference 2). How does the RFID tag modulate its data on the carrier frequency it sends back to the reader? Again, there’s no consistent strategy. AM (am-

plitude modulation)—specifically ASK, or amplitude-shift-keying, FM (frequency modulation), phase modulation, and PWM (pulse-width modulation) are all possibilities. To minimize the probability that two tags may simultaneously broadcast, thereby corrupting each other’s signals, manufacturers sometimes employ TDMA (time-division-multiple-access) algorithms. Infineon’s 13.56-MHz, PJM (phase-jitter-modulation) RFID tags employ modulation techniques the company licensed from Magellan Technology. The techniques reportedly enable the tags to read and write at rates as high as 848 kbps—approximately 25 times faster than conventional 13.56-MHz tags; they also implement FTDMA (frequency- and time-division-multiple-access) and eight-channel frequency-hopping for anticollision-interference avoidance (Table 1).

CRC (cyclic-redundancy check) or other checksum codes can determine whether the reader correctly received a tag’s transmission, and a plethora of ECC (error-correcting-code) schemes can correct bad bits and prevent the need for time-consuming rescanning. Currently, no consistency exists about whether the broadcast data is encrypted, although large implementers, such as Wal-Mart, are driving de facto standards and beginning to bring some order to the morass. Whether you choose to implement encryption in your design and how robust that encryption is can significantly affect the tag’s cost, size, power draw, and other key factors.

One key advantage that RFIDs have over bar codes is that individual units can contain unique identifying data sequences; UPC codes, conversely, are

TABLE 1—COMPARISONS OF VARIOUS RFID APPROACHES

	Low frequency	High frequency		Ultrahigh frequency	Microwave
Frequency	125 to 134 kHz	13.56 MHz	JM 13.56 MHz	866 to 915 MHz	2.45 to 5.8 GHz
Market share*	74%	17%	Introduced 2003	6%	3%
Reading distance	As far as 1.2m	As far as 1.2m	As far as 1.2m	As far as 4m**	As far as 15m***
Speed	Not so fast	Medium	Very fast	Fast	Very fast
Wet environment	No influence	No influence	No influence	Bad influence	Bad influence
Orientation of transponder to reader necessary	No	No	No	Partly	Yes
Worldwide-accepted frequency	Yes	Yes	Yes	Partly (European Union, United States)	Partly (not European Union)
Existing ISO standards	11784/85, 14223	18000-3.1/15693, 14443 A, B, and C	18000-3/2	EPC C0, C1, C1G2	18000-4
Major applications	Access, immobilizer, gas, laundry	Library, item tracking, pallet, transportation	Airline, postal, pharmaceutical, cigarettes	Pallet, truck, trailer, tracking	Road toll, container

*Venture Development Corp report 2002, worldwide shipment of RFID transponders (units)

**In the United States

***Active (with battery)

(Courtesy Infineon)

generic to all units of a manufacturer's product. And, if rewritable memory, such as EEPROM, flash memory, battery-backed RAM, FRAM, or MRAM, contains the EPC (electronic product code), you can alter and append the EPC as the item goes through its manufacturing, distribution, sales, and usage life. How much data the RFID should store is a topic of much debate, and is to some extent application-driven. STMicroelectronics' XRA00 UHF RFIDs, for example,

support EPCglobal Class 1 specifications. They contain a 128-bit memory organized as eight blocks of 16 bits each. The first block stores a 16-bit CRC value. The next six blocks store the 96-bit product code that the device uses during the inventory sequence, and an 8-bit "kill code" and eight lock bits that protect the memory contents share the last block.

Under the EPCglobal scheme, the RFID reader, after reading the EPC code from the tag, queries ONS (Object Nam-

ing Service) servers whose databases VeriSign administers. These servers, conceptually analogous to the DNS (Domain Name Servers) that translate URLs (uniform resource locators) into IP (Internet Protocol) addresses, return the IP address of a server that contains detailed information on the RFID-tagged item. EPCglobal, an outgrowth of the earlier Auto-ID Center, is one of two primary RFID standards-setting groups; the ISO (International Organization for Standard-

PRIVACY CONCERNS



RFID technology's cost and other benefits to suppliers—and, there-

fore, the price and other benefits to consumers—are apparent throughout the manufacturing, distribution, and sales processes, right up to when a cashier rings up the RFID-tagged item at the register. Beyond that point, if the RFID remains active, the benefits to consumers become more ambiguous, and the potential downsides, particularly as they relate to privacy, become more ominous.

The Wikipedia Web site, within its definition of RFID (www.wikipedia.org/wiki/RFID), includes a comprehensive summary of RFID's privacy issues, which the following list summarizes:

- The purchaser of an item will not necessarily be aware of or able to remove the tag;
- An RFID reader can read the tag at a distance without the knowledge of the individual;
- If a purchaser pays for a tagged item with a credit card or loyalty card, then the store could tie the unique ID of that item to the identity of the purchaser; and
- Tags create or may later create globally unique serial numbers for all products, even though this fact creates privacy problems and is unnecessary for most applications.

Standards-based RFID specifications include the ability to send a "kill" command to the tag.

However, with current RFID-tag and -system designs, consumers have no guarantee and no indication of whether the system has sent the command. And consumers might not even view a permanently killed tag as a desirable outcome. In a UPC (universal product code)-free world, the EPC (electronic product code) might be a key part of the rebate process, for example, and it could find use when someone returns an item for refund. In this case, the store would have to replace the killed tag before returning the item to the sales floor.

A retailer can now use UPC and other information, along with your credit-card number, to precisely connect you to items you've purchased at the retailer's store. However, a global RFID database could potentially enable that retailer to extend that insight to items you've acquired elsewhere. That reach could extend to other activities: What could an RFID tag embedded in your passport, driver's license, license plate, or on your body reveal? Government agencies would, of course, have similar visibility with similar potential for both positive use and abuse. And how would you feel if a stranger, with a precision, high-gain antenna and sufficient DSP horsepower, could park outside your home and scan and analyze its RFID-tagged contents?

Some pundits believe that RFID critics exaggerate privacy

fears because the high costs of RFIDs restricts their use to multi-item, not individual, cases. This stance seems naive in the face of years' worth of Moore's Law-driven cost-reduction trends. Also keep in mind that, for large items, such as computers and televisions, there is only *one* case. Other pundits claim that RFID is just the latest in a long line of technologies whose unveiling instigated a chorus of concern, but whose benefits eventually outweighed the downsides. RFID may be different, though. Once manufacturers implement it, we cannot turn back, and, even with legislative oversight, the checks and balances in the system to prevent abuse seem, at best, tenuous.

Some analysts point out that consumers have thus far been apathetic and careless about their privacy and are happy to sell their identities for free gifts, store discounts, and the like. Although these observations may hold some truth, one important distinction exists. In the past, consumers have consciously chosen to give up their privacy. They do so whenever they swipe their supermarket discount card, fill out and send a Web-site form, or mail in a rebate or registration card. With RFID, consumers cannot make that choice; monitoring occurs regardless of whether they have approved it.

At this year's Blackhat Conference in Las Vegas, Lukas

Grunwald, a senior consultant with DN-Systems Enterprise Solutions GmbH, unveiled the RFDump program, which showed just how easily anyone with a reader can access and alter RFID-tag contents. Tag cracking should be of concern to both consumers and retailers: Why bother shoplifting when you can, armed with a handheld computer, an RFID-reader add-in card, and a copy of RFDump, reduce the price of that new jacket from \$100 to \$25? And the potential exists for illicitly scanning a home from the sidewalk, despite RFID's claimed inches-to-feet frequency-dependent maximum range. Remember that 802.11 signals that once extended only a few yards now can span multiple-mile distances, thanks to increasingly sophisticated signal-processing and error-correction algorithms, along with low-tech Pringles cans, which concentrate the signal's energy in a focused direction.

For more information on the privacy issues surrounding RFID and on advocacy efforts to increase consumer awareness and influence private and public policy concerning RFID, visit the following Web sites: the ACLU (American Civil Liberties Union, www.aclu.org), CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering, www.nocards.org), and the EFF (Electronic Frontier Foundation, www.eff.org).

ization) is the other. Clearly, the two groups need to collaborate their data-format-conforming efforts for RFID to become truly ubiquitous. On the other end of the memory-density spectrum are companies such as Boeing, which is test-

ing much larger, 10-kbit RFID tags that enable the storage of long serial numbers, detailed parts information, and repair histories. The large-RFID-tag approach also applies whenever an RFID reader is not connected to a network and, there-

fore, cannot access the ONS in real time.

Another important advantage of RFIDs over bar codes is that laser line-of-sight orientation between a tag and a reader is unnecessary. Any alignment between tag and reader is also *potentially* ir-

APPLICATION TEASERS



The following list includes some of the more interesting applications for RFID. They might inspire you to use RFID technology in your future designs and increase your awareness of the privacy issues associated with RFID.

- Wal-Mart's challenge to its suppliers, which it first issued at the June 2003 Retail Systems Conference in Chicago, was the key spark that ignited significant industry momentum behind RFID. Pilot implementations with key suppliers are under way at Wal-Mart's Sanger, TX, distribution center and seven Dallas/Fort Worth-area stores. Wal-Mart's top 100 suppliers have until next January to install tags on items headed for three Texas distribution centers. By June 2005, Wal-Mart expects to have its RFID project live in as many as six distribution centers and as many as 250 Wal-Mart and Sam's Club locations. By January 2006, the next 200 suppliers are scheduled to join the initiative. Wal-Mart's competitors have responded by launching their own RFID trials.

- The US government, motivated by homeland security, inventory tracking, and other concerns, is another significant catalyst for RFID action. Department of Defense suppliers must by next January begin using RFID on portions of their inventory. The Department of Transportation's Federal Highway Administration has also called on RFID manufacturers to jointly develop DSRC (dedicated short-range-communications) systems as part of the agency's efforts to halve road fatalities in the United States within 10 years. Potential roadway appli-

cations include issuing alerts to drivers about impending intersection collisions, rollovers, and weather-related road hazards and warning drivers that their vehicles are traveling too fast to safely negotiate an upcoming curve. The FCC in 1999 allocated the entire 5.9-GHz band to DSRC applications. The State Department is conducting a trial of RFID-inclusive biometric passports, with an eye toward moving to full production in 2005. (The International Civil Aviation Organization has unveiled a similar proposal, with a 2015 deadline.) And the Customs Service's CSI (Container Security Initiative) and SST (Smart and Secure Trade) Lanes Initiative are embracing RFID technology as a way to help ensure container security at US ports. To date, the governments of the top 20 foreign ports, representing approximately two-thirds of the volume of shipments to the United States, have agreed to implement CSI and SST.

- Governments outside the United States are also evaluating and implementing RFID. Persistent rumors suggest that the European Union is planning to embed RFID tags in high-value euro notes. (Rumors of RFID tags embedded within US \$20 bills, conversely, are unfounded.) The United Kingdom is also studying license plates with embedded RFID tags, which readers can decipher from 300 feet away and readers embedded in the road or surveillance vehicles can decipher in rapid succession. And electronic ear-tagging of sheep and goats, fueled by "Mad Cow"-Disease outbreaks, will be compulsory in Europe beginning in January 2008 for member states with livestock

populations of 600,000 or more. ISO 11784/85 also stipulates that it will be compulsory for animals intended for inter-European Union trade; domestic-RFID-supplier Philips has been particularly active in this area. Canada will also implement electronic tagging of livestock next January.

- Significant RFID implementation potential exists in the pharmaceutical industry to track drugs (likely extending to individual packages, not just bulk cases) and prevent counterfeiting, unintended redirection, and theft.

- E-Zpass and FasTrak systems implement electronic-highway-toll collection. Those concerned about privacy should note that they can log not only your preferred payment method, but also the dates, times, and locations your car's RFID tag passed readers. Other RFID-based electronic-payment systems include ExxonMobile Speedpass, MasterCard's PayPass, NCR's FastLane system, and FreedomPay. Nokia has unveiled its first RFID-inclusive cell phone add-in kit for electronic item payment, the Mobile RFID Kit for the model 5140. And Nokia, Philips, and Sony have formed the RFID-derived Magic Touch alliance for mobile commerce and information exchange.

- Many of you are likely familiar with the "chipping" programs from such companies as Avid and HomeAgain for identifying pets and returning them to their owners. This scenario is extending to humans. The Mexican government recently used technology from VeriChip to subdermally tag Mexico's Attorney General Rafael Macedo de la Concha, along with 160 of his employees working at an anticrime information center in

Mexico City. Other places in Central and South America are employing the technology in response to escalating incidents of "flash kidnapping," involving short amounts of time in captivity. And at the Baja Beach Club in Barcelona, barely clothed patrons who don't want to carry currency are sporting subdermal tags to enable electronic "credit-card" payment of food and drinks.

- Japanese primary schools in Osaka and Tabé are tagging students' clothing, bags, and name-tags, so that teachers and parents can track the children's whereabouts. For similar reasons, the Wannadoo City theme park in Florida is tagging all ticket holders upon entry, so that members of each group can find each other in real time. Premium Club Seat ticket holders at the Seattle Seahawks' Qwest Stadium can use RFID-inclusive PowerBuy tags that reduce their time in line at concession stands. Texas Instruments is both an RFID supplier and an RFID consumer, and it employs RFIDs for tracking work in progress within its fabs. And 2004 Olympic Marathon and Boston Marathon participants' shoes contained RFID tags, which communicated at regular intervals with readers embedded in the pavement or within mats on the raceway. These tags not only prevent Rosie Ruiz-reminiscent fraud, they conceptually also could allow runners' friends, families, and fans to follow race progress through periodic Web-site updates, pager alerts, and the like.

- Texas Instruments has also worked with the Vatican Library in Rome to RFID-tag, identify, and manage its extensive collection of nearly 2 million books, manuscripts, and other priceless items.

relevant because proximity requirements depend on which antenna technology you employ. Circular-polarized antennas, like omnidirectional microphones, emit and receive radio waves in a circular pattern. Using them provides a better chance that the destination will receive a broadcast signal in situations in which the sender cannot precisely control the orientation between the transmitter and the receiver. Conversely, the operating range of a circular-polarized antenna system is less than that of a linear-polarized antenna, which is analogous to a unidirectional microphone.

ISSUES=OPPORTUNITIES

US journalist, attorney, and motivational writer Napoleon Hill (1883 to 1970), the so-called Founder of The Science Of Success, stated that “Every adversity, every failure, every heartache carries with it the seed of an equal or greater benefit.” Keep that quote in mind as you survey today’s seemingly irreconcilable RFID landscape; sooner or later, it will inevitably sort itself out, and the companies that guess right will greatly benefit from that consolidation (see sidebar “Application teasers”). Aside from speed-boosting modulation schemes, such as Infineon’s PJM, several other RFID-tag-differentiation opportunities exist. They include size, as Hitachi’s 2.45-GHz μ -Chips exemplify. The chips, which contain embedded antennas, measure only 0.3 mm sq (Figure 1). Other differentiators include power consumption and communication robustness. (One factor currently limiting the adoption of RFID is that, in some field trials, it’s no more reliable to read than are bar codes.)

Companies are also investigating various means of supplementing traditional-RFID functions with environmental sensors that can report such factors as tire pressure; temperature; humidity; the presence of various biological agents to determine contamination, spoilage, and the like; and whether someone has previously tampered with or mishandled the item by using excessive force or vibration, for example (Reference 3). The tag can report real-time data; alternatively, it can provide a simpler indication that the measurement has at some point exceeded a threshold value. Cost is, of course, perhaps the most im-

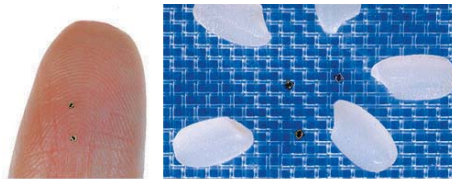


Figure 1 A fingertip dwarfs Hitachi’s μ -Chips, which are a fraction of the size of a grain of rice (courtesy Hitachi).

portant improvement factor that will broaden RFID’s applicability. It makes little sense to attach an RFID tag to an item whose cost is comparable with or even within one or two orders of magnitude of the cost of the tag itself. For example, although a retailer may today be interested in RFID-tagging large cases of paper towels, RFID costs will have to significantly drop before the retailer will consider tagging individual paper-towel rolls. This cost-driven brake on adoption will, at least in the short term, act as a natural means of addressing RFID-privacy concerns.

The long-term potential for RFID ubiquity is bright, but the size and cost pressures that will increasingly affect tags lead to uncertain prospects that they’ll fill many semiconductor fabs or that they’ll be wildly profitable for their manufacturers. Why, then, are so many people so excited about RFID? The reason is simple: The worth of all of that data streaming off RFID tags and readers, in and of itself of little value, emerges when other hardware and software on the Internet or a company’s Intranet stores, transports, and manipulates the data. As a result, many will benefit—CPU vendors, such as

AMD, IBM, Intel, and Sun; their sibling systems divisions; systems partners, such as Apple, Dell, and HP; networking-equipment vendors, such as Cisco; and enterprise-software suppliers, such as Microsoft, Oracle, and SAP. The storage, transportation, and manipulation of that data also drives the fact that much of the recent media coverage of RFIDs has appeared in IT publications (see sidebar “Additional insights”). This data explosion will, of course, also enrich the fortunes of DRAM, hard-disk-drive, Ethernet, and other system-building-block suppliers.

For those designing RFID readers or implementing readers that others developed, the diversity of frequencies, formats, modulation, interference-suppression schemes, and other variables may motivate you, if your customers’ cost expectations allow, to make those readers as flexible as possible. For the readers’ digital subsystems, you can ensure flexibility primarily by enabling updatable firmware using code storage in flash memory or a small-form-factor hard-disk drive instead of ROM and by enabling updatable

hardware using FPGAs and PLDs rather than ASICs. With the RFID readers’ analog subsystems, you might consider implementing programmable analog arrays from companies such as Anadigm, Lattice Semiconductor, and Zetex, instead of hard-wired circuits (Figure 2). □

RFID costs will have to significantly drop before the retailer will consider tagging individual paper-towel rolls.

REFERENCES

1. Dipert, Brian, “Pick a card,” *EDN*,

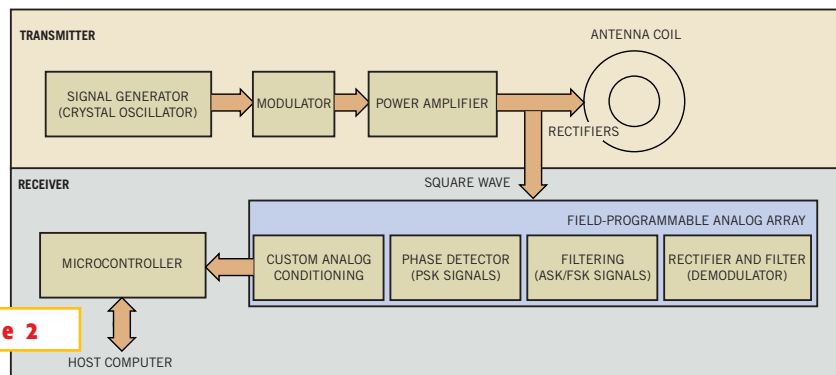


Figure 2 Replacing hard-wired functions with a programmable analog array results in a more format-flexible RFID reader (courtesy Anadigm).

July 8, 2004, pg 53.

2. Dipert, Brian, "Running interference," *EDN*, Aug 22, 2002, pg 24.

3. Marsh, David, "Safety check: Wireless sensors eye tire pressure," *EDN*, Sept 2, 2004, pg 42.

AUTHOR'S BIOGRAPHY



Technical Editor Brian Dipert wonders about the significant and long-term privacy impacts of RFID. What do you think? Reach him at 1-916-454-

5242, fax 1-617-558-4470, bdipert@edn.com, and www.bdipert.com.

TALK TO US

Post comments via TalkBack at the online version of this article at www.edn.com.

FOR MORE INFORMATION...

For more information on products such as those discussed in this article, contact any of the following manufacturers directly, and please let them know you read about their products in *EDN*.

Airbus
www.airbus.com

Albertsons
www.albertsons.com

AMD (Advanced Micro Devices)
www.amd.com

Anadigm
www.anadigm.com

Apple Computer
www.apple.com

Avid (American Veterinary Identification Devices)
www.avidid.com

Best Buy
www.bestbuy.com

Boeing
www.boeing.com

Cisco Systems
www.cisco.com

Dell
www.dell.com

Delta Airlines
www.delta.com

EPCglobal
www.epcglobalinc.com

ExxonMobile
www.exxonmobile.com

E-ZPass
www.ezpass.com

FasTrak
www.511.org/fastrak/

Federal Express
www.fedex.com

FreedomPay
www.freedompay.com

Hewlett-Packard
www.hp.com

Hitachi
www.hitachi.com

HomeAgain
www.homeagainid.com

IBM (International Business Machines)
www.ibm.com

Infineon Technologies
www.infineon.com

Intel
www.intel.com

ISO (International Standards Organization)
www.iso.org

Kroger
www.kroger.com

Kureha Kankyo
www.kurekan.co.jp

Lattice Semiconductor
www.latticesemi.com

Magellan Technology
www.magtech.com.au

Marsh
www.marsh.net

MasterCard International
www.mastercard.com

Metro Group
www.future-store.org

Microsoft
www.microsoft.com

NCR
www.ncr.com

Nokia
www.nokia.com

Oil ID Systems
www.x-changeCorp.com

Oracle
www.oracle.com

Philips
www.philips.com

SAP
www.sap.com

Sony
www.sony.com

STMicroelectronics
www.st.com/contactless

Sun Microsystems
www.sun.com

Target
www.target.com

Texas Instruments
www.ti.com/tiris

VeriChip
www.adsx.com

VeriSign
www.verisign.com

Wal-Mart
www.walmart.com

Zetex
www.zetex.com