Design of Ultra-Low-Cost UHF RFID Tags for Supply Chain Applications

Rob Glidden, Cameron Bockorick, Scott Cooper, Chris Diorio, David Dressler, Vadim Gutnik, Casey Hagen, Dennis Hara, Terry Hass, Todd Humes, John Hyde, Ron Oliver, Omer Onen, Alberto Pesavento, Kurt Sundstrom, and Mike Thomas, Impinj, Inc.

ABSTRACT

The availability of inexpensive CMOS technologies that perform well at microwave frequencies has created new opportunities for automated material handling within supply chain management (SCM) that will, in hindsight, be viewed as revolutionary. This article outlines system architecture and circuit design considerations that influence the development of radio frequency identification (RFID) tags through a case study involving a high-performance implementation that achieves throughput of nearly 800 tags/s at a range greater than 10 m. The impact of a novel circuit design approach ideally suited to the power and die area challenges is also discussed. Insights gleaned from first-generation efforts are reviewed as an object lesson in how to make RFID technology for SCM, at a cost measured in pennies per tag, reach its full potential through a Generation 2 standard.

INTRODUCTION

HISTORY

Radio-based identification has appeared in a variety of diverse forms — from keyless entry badge readers, to automatic toll collection, to smart cards — over the past decade. However, radio frequency identification (RFID) has been around much longer, tracing its roots to military identification friend or foe (IFF) systems that appeared during the Second World War, at about the same time as radar. Later, the technology was used for railroad car and military asset tracking, and even livestock management through tag implants.

RFID systems are often classified as passive (deriving power in the tag solely from rectifying the incident RF power) or active (battery-assisted). Many of these systems are based on a low-frequency standard at 13.56 MHz, with read distances on the order of 1 cm. Longer-range systems often use high transmitted power, higher frequencies, and/or active or semi-passive transponders for range enhancement. A key difference among systems involves the physics of the air interface; low-frequency systems, with their long wavelength energy, tend to communicate in the electromagnetic near field, whereas microwave systems deal with radiated energy in the far field. In the former case, sensing occurs from detecting the load on a transformer primary in the presence of a "secondary winding" (the tag), whereas far field sensing involves changing the tag's radar cross-section, effectively modulating the return echo of a continuous wave (CW) signal originating at the reader. In fact, microwave RFID systems strongly resemble Doppler radars.

COMMERCIAL SIGNIFICANCE

RFID is poised to move into a new class of high-volume uses that will cause this technology to become ubiquitous. Made possible by the Internet and its underlying information infrastructure, it is actually not the tag or reader that is the significant development, but rather the information itself — about the location and status of goods worldwide, to manufacturers, distributors, and retailers simultaneously — that makes RFID an enabling technology. This has become the motivation for retailers such as Wal-Mart, as well as the U.S. Department of Defense, to mandate the use of RFID by their top suppliers beginning in 2005.

Typical scenarios for this application of RFID are illustrated in Fig. 1. Goods can be automatically marked and inventoried in many real-time situations, including manufacturers' conveyor lines, loading and unloading of trucks at dock doors, and handling palletized loads within warehouses or distribution centers. Labor savings from avoidance of manual bar code scanning or keypad entry makes RFID attractive for this use alone.

However, bar code replacement is just the beginning, and the real economic benefits come from higher-level uses [1]. These include theft and loss prevention, streamlined inventories, reduced turnaround time, and avoidance of unnecessary handling. More sophisticated use involves production adjustment in response to inventory levels as manufacturers gain access to real-time information on products further down-

0163-6804/04/$20.00 © 2004 IEEE

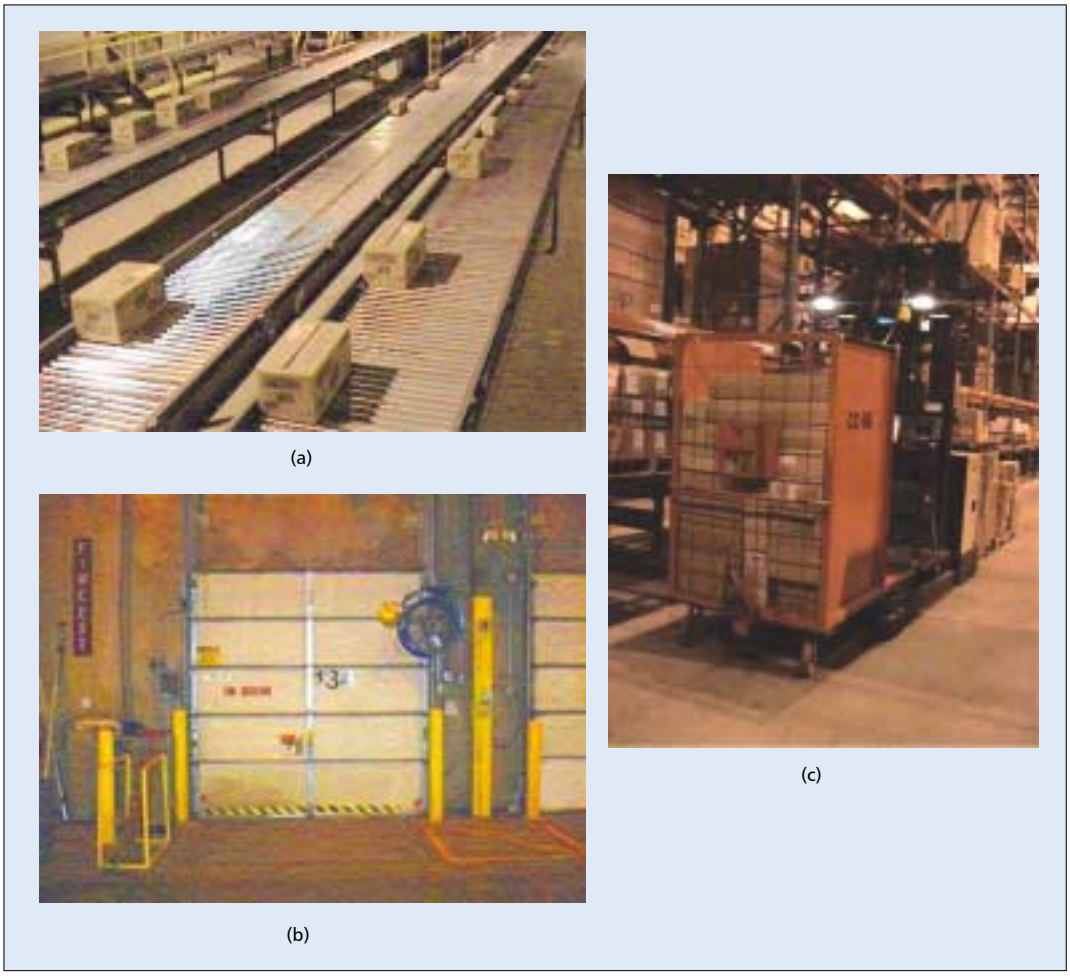

Figure 1. *RFID application scenarios; a) conveyors; b) dock doors; c) fork lifts and palletized goods.*

Systems must be foolproof and robust, building on existing business processes that are today centered on optical bar codes governed by the UPC format, even as RFID overcomes several limitations of bar codes.

stream, and even to take responsibility for replenishing goods on demand at the distribution center or retail store level. Thus, while the impetus for RFID is coming from retailers to benefit distribution efficiencies, there is also the expectation that manufacturers will become more efficient and improve their own productivity, further lowering product cost to the retailer.

Standards

Moving into the UHF frequencies to exploit range benefits through use of unlicensed industrial, scientific, and medical (ISM) bands has led to the creation of several first-generation protocol standards. Two of these trace to the leadership of the Auto-ID Center at Massachusettes Institute of Technology (MIT), an organization that recognized the potential of RFID early on [2, 3]. Other standards originated with the International Standards Organization (ISO) as part of the ISO 18000 family, with the -6 group of documents dedicated to UHF operation. Generally, these standards originated from proprietary protocols advanced by individual suppliers.

Table 1 compares the major attributes of the significant UHF standards. Widely differing approaches to modulation format and functionality have been taken, and debate over the "best" format continues. Nonetheless, these are all first-generation efforts that resolve trade-offs narrowly, and in hindsight there is no single approach that is a good fit for all user requirements across a broad range of scenarios, considering feature sets, communication robustness, regulatory environment, and read rates.

System Requirements and Trade-offs

The User's Perspective

RFID systems for the supply chain emphasize tagging of pallets, cases, and in certain situations individual items [4]. End users view tags merely as a vehicle for data collection, and readers as the collection point. Systems must be foolproof and robust, building on existing business processes that are today centered on optical bar codes governed by the universal product code (UPC) format, even as RFID overcomes several limitations of bar codes:

- Bar codes require optical line of sight, and are blocked by many materials that are transparent to RF.
- Bar codes are fixed at the time of printing.
- Bar codes can be rendered useless by defacement or smudging.
- Bar codes can be spoofed or easily defeated by any malicious individual having a laser printer at their disposal.

Key parameters	Auto-ID Class 0	Auto-ID Class 1	ISO 18000-6 A	ISO 18000-6 B
Forward link				
Operating frequency	902 MHz–928 MHz	902 MHz–928 MHz	860 MHz–930 MHz	860 MHz–930 MHz
Air interface	AM pulse width mod.	AM Pulse width mod.	Pulse interval ASK	Manchester ASK
Bit period	NA: 25 μs/12.5 μs EU: 62.5 μs	NA: 14.25 μs EU: 66.67 μs	Data '0': 20 μs Data '1': 40 μs	125 μs/25 μs
Data rate	NA: 40/80 kb/s	NA: 70.18 kb/s	33 kb/s (1)	8/40 kb/s[1]
Worst case Duty cycle:	52% Data '1' low for 6 μs	62.5% Data '1' low for $3T_0/8$	50% Data '0' low for 10 μs	50% Manchester code
Modulation depth [min, max]	[20%, 100%]	[30%, 100%]	[27%, 100%]	Nom 15%: [13%,17%] Nom 99%: [90%, 100%]
Reverse link				
Air Interface	Passive Backscatter: FSK	Passive Backscatter: Pulse Interval AM	Passive Backscatter: Bi-Phase Space AM	Passive Backscatter: Bi-Phase Space AM
Bit period	NA: 25 μs/12.5 μs EU: 62.5 μs	NA: 7.13 μs EU: 33.33 μs	25 μs	25 μs
Data Rate	NA: 40/80 kb/s EU: 16 kb/s	NA: 140.35 μs EU: 30/00 kb/s	40 kb/s[1]	40 kb/s[1]
Forward-to-reverse link turnaround	Not applicable[2]	NA: 114 μs	Shall not exceed 100 μs	Shall not exceed 100 μs
General				
Reset signal duration	800 μs (CW)	64 μs (CW)	300 μs (CW)	400 μs (CW)
Collision arbitration	Deterministic binary tree search	Deterministic/Slotted	Adaptive	Probabilistic binary tree search
Tag read speed	Nom: 200 tags/s Max: 800 tags/s	Not specified	Nom: 100 tags/sec (~l0 ms/tag)	Nom: 100 tags/see (~l0 ms/tag)
Tag capacity	Not limited by standard	~300[4]	~300[4]	~300[4]
Memory				
Memory type	Read-only	User programmable	User programmable	User programmable
Memory organization	EPC: 64/96 bits Kill Code: 24 bits Total: >= 120 bits	PC: 64/96 bits Kill Code: 8 bits Total: >= 104 bits	Up to 256 blocks w/256 bits/block (2 kb)	Up to 256 blocks w/8 bits/block (2 kb)
Security/privacy				
Features	Moderate IDO/ID1 + 24 bit kill passcode	None Reader broadcasts all or part of ID code. Reader can request kill passcode.	None Reader broadcasts UID/ SUID. Production set block lock bits. No kill command.	None Reader broadcasts UID/SUID. Production set block lock bits. No kill command

[1] No mention of data rates specific to European operation. Reverse link is always 40 kb/s.

[2] For Auto-ID Class 0, the tag data response is always known a priori (i.e., nothing has to be computed based on the current bit).

[3] Probabilistic collision arbitration implies that tag selection speed will depend on the tag population size. This is a disadvantage.

[4] These standards are limited by the probabilisitic nature of their collision arbitration protocols. Most of them assume a tag population

Table 1. *First-generation UHF standards for RFID.*

RFID can thus lead to more complete automation of material handling, with greater overall efficiency.

Unique identifiers ensure no ambiguity; using a 96-bit electronic product code (EPC) field corresponds to 10^{29} objects, which is approximately 2×10^{19} for every human now alive. This provides absolute uniqueness many orders of magnitude greater than the UPC system, again offering opportunities for traceability of goods not otherwise possible.

Regulatory Environment

Widespread deployment of RFID relies on availability of either dedicated or unlicensed ISM bands. Current interest is in the UHF frequencies, which offer a good balance between antenna size and path loss. However, the requirements for these bands vary widely around the world, frustrating attempts to deploy systems in an era of global trade.

North America — In the United States, the FCC provides unlicensed spectrum in the 902–928 MHz band, as governed by Part 15, Section 247 regulations. These rules permit radiated power up to 1 W total, 4 W effective isotropic radiated power (EIRP). For electromagnetic interference mitigation, spread spectrum techniques are used, either direct sequence or frequency hopping, with channel separation of 25 kHz and out-of-channel emissions 20 dB down in the latter case. Since emissions limits govern the primary transmitter, when applied to RFID these regulations do not directly address backscatter emissions of passive tags.

Europe — With a more crowded electromagnetic environment, regulations in Europe are far more constraining, effectively limiting the range of RFID systems. Currently, European Telecommunications Standards Institute (ETSI) EN 300 220-1 and European Radio Communications Committee (ERC) Recommendation 70-03 govern such systems, providing a very narrow band of frequencies across 869.4–869.65 MHz. In contrast to FCC rules, the entire 250 kHz band may be allocated to a single channel, but radiated power is restricted to 500 mW. As in the United States, regulations do not directly address backscatter emissions, but duty cycles are limited to less than 10 percent.

In recognition of the need for greater spectrum allocation, proposed changes are under consideration, with pending regulations governed by Draft ETSI EN 302 208-1 v1.1.1 (2003-12). These rules open the spectrum from 250 kHz to 3 MHz, covering the band 865–868 MHz with channel spacing of 200 kHz. Other significant changes include the definition of spectral masks for both reader and tag emissions, and multiple power classes, recognizing the potential for interference with critical uses at the band edges. These classes include:
Power class 11: 100 mW ERP (865–868 MHz)
Power class 12: 500 mW ERP (865.6–868 MHz)
Power class 13: 2.0 W ERP (865.6 –867.6 MHz)

Asia — Japanese UHF RFID spectrum regulations are not fully defined at this time. The Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPMHAPT) is investigating UHF band RFID spectrum allocation, with a temporary allowance in the band of 950–956 MHz. Preliminary information suggests use of frequency-hop spread spectrum techniques with channelization of 1 MHz, a duty cycle limit of 16.67 percent, reader out-of-band emissions of –36 dBm, and no regulation of tag emissions. Limits on radiated power have not yet been established, and it is probable that RFID uses of spectrum will be reconsidered at some future date.

Similarly, RFID regulations in China and Korea are in transition. Currently, neither China nor Korea permits the use of the spectrum for RFID purposes or for other short-range devices, but both countries are showing interest in the technology. China is now considering use of spectrum at 433 MHz for active RFID and close to 900 MHz for passive RFID usage, with tentative regulations expected before the end of 2004. Likewise, Korea is likely to commit spectrum for RFID at 433 MHz and 910–914 MHz bands in the coming year.

Given often conflicting global constraints, with the implied requirement to recognize tags wherever goods might flow, the challenge is to build in support for multiple data rates, modulation formats, and interference environments through a flexible and programmable air interface.

Link and Power Budgets

In passive backscatter systems, range is often set by the forward link through the radiated power available at the tag. Theoretical range is determined from the Friis equation:

$$R \le \frac{\lambda}{4\pi}\sqrt{\frac{EIRP_{reader}G_{tag}}{P_{tag}}},$$

where P_{tag} is power required at the tag antenna output, G_{tag} is the tag antenna gain, and λ is the wavelength of the RF carrier.

With only microwatts to work with at the tag antenna and rectifier efficiencies on the order of 20 percent, tag circuits must operate from only a few microamps of current at under a volt:

$$P_{tag} = \frac{K_{loss} \times I_{load} \times V_{load}}{\eta_{rectifier}},$$

where K_{loss} is the modulation loss parameter and $\eta_{rectifier}$ is the power conversion efficiency.

Power in the return link accessible to the reader frontend is on the order of –25 to –65 dBm, which is easily detectable by inexpensive means.

Protocol

Signaling across the air interface represents a careful balance between communications efficiency and RF power loss at the tag rectifier through modulation. Amplitude modulation or equivalent approaches are regularly used to simplify detection of the forward link signal. This avoids the power burden of circuits required for coherent detection with frequency or phase modulation, but comes at the cost of power loss during symbol transmission.

Field Rewritability

Uniqueness of EPC data means that every chip must be personalized during the manufacturing process. In some cases, it is also desirable to write user information into the tag while in service. Uses include timestamping, expiration dates for goods with limited shelf life such as pharmaceuticals, or real-time data such as in

Given often conflicting global constraints, with the implied requirement to recognize tags wherever goods might flow, the challenge is to build in support for multiple data rates, modulation formats, and interference environments through a flexible and programmable air interface.

We have created an implementation of a first-generation standard, known as the Zuma RFID™ design. The name derives from a popular, trend setting California beach, with the beach theme symbolic of countless individual grains of silicon.

baggage handling. User data can greatly relieve network traffic to central database servers when tag information is locally relevant. User data also opens the possibility for more efficient tag identification and sorting.

Integrated Circuit Challenges

Building a commercially viable passive RFID tag can be a difficult task. The challenges are many and varied, and in many ways different from other semiconductor products.

Power Management

As with digital watches, hearing aids, and pacemakers, which must operate over long periods on a very limited power source, RFID chips are best implemented using complementary metal oxide semiconductor (CMOS) technology. Unlike those applications, however, tag power varies by roughly three decades from minimum to maximum range. This variability creates one of the most challenging situations for power supply predictability, and rejection of transient phenomena, in integrated circuit design. The problem is not limited to power dropouts; in fact, at short distances it is possible to put sufficient power into the tag to induce electrical overstress.

Nonvolatile Memory

Personalizing each tag uniquely requires some form of nonvolatile storage, whether laser trimmed at the time of manufacture, one-time programmable, or electrically rewritable. Rewritable nonvolatile memory is clearly preferred for achieving high throughput during production test, and concurrently offers the benefit of user memory.

ESD

During assembly of the silicon chip to the corresponding label, ESD damage can be of great concern. Many of the materials used are known to produce high levels of triboelectric charge, and large potentials can be produced in the manufacturing environment. Making matters worse, conventional techniques for circumventing this built-up charge can radically degrade the RF performance of the input ports through the addition of large parasitic capacitances. These capacitances not only frustrate the antenna design, forcing it to be highly inductive, but also affect the rectifier conversion efficiency and form a potentially unacceptable source of power loss.

Die Area

Tagging consumer products at the case and item level demands an applied cost measured in pennies [5]. This requirement goes beyond the cost of the silicon alone, and the silicon is actually not the dominant expense if done well. While many factors influence overall cost at the die level, including process complexity, maturity, yield, and robustness, the economics of RFID for supply chain applications generally fail for die areas exceeding 1 mm^2. Area efficiency has traditionally been important in integrated circuit design, but takes on new meaning when trying to shoehorn a complete communications transponder with hundreds of bits of memory, thousands of gates of logic, and companion analog functions such as modems and power regulation on a single substrate.

Test Approach

Along with die area, test cost is a major economic driver for RFID. Consider the use of conventional VLSI testers, with costs on the order of $0.10/s (inclusive of operator labor and equipment depreciation), making test costs alone potentially comparable to the product's entire applied cost!

Implementation

We have created an implementation of a first-generation standard, known as the Zuma RFID™ design. The name derives from a popular trend-setting California beach, with the beach theme symbolic of countless individual grains of silicon. In fact, the Zuma chip is about the size of a grain of sand, but represents a high level of very large-scale integrated (VLSI) functionality. The first-pass functional chip is manufactured in an industry-standard 0.25 μ logic CMOS process, and implements the Class 0 protocol [6], which we chose based on the success of the approach in previous field trials and our assessment of technical advantages of the air interface. The chip also includes user memory and has the capability to perform field writes, providing for the first time a way to personalize the information-bearing content of RFID tags while simultaneously achieving considerably smaller die area. These benefits derive from a novel circuit approach that perfectly fits the unique requirements of RFID.

Self-Adaptive Silicon Approach

We have learned that various circuits can be more effectively implemented in standard CMOS processes with a fraction of the space and power needed by conventional circuit topologies. This comes through rethinking the physics of floating-gate MOSFETs [7, 8]. Floating gates are typically associated with Flash or EEPROM nonvolatile memory (NVM) technology, which adjusts the electronic charge on an *n*-channel FET floating gate to store one of two digital values. Our approach, termed *self-adaptive silicon* (SAS), differs radically from traditional floating gate technology in two fundamental ways [9–11]:

- We fabricate floating gate devices in standard digital CMOS, with no additional process steps or mask layers.
- The floating gate MOSFET remains a fully functional transistor during programming or tuning, allowing us to store precise analog values on the floating gate. This leads to the concept of analog memory elements that are a superset of binary-state memories, yet SAS has application to ultra-low power high-performance RFID tags beyond memory alone, notably in overcoming manufacturing tolerances of analog circuit parameters [12].

SAS allows electrically tunable transistors with permanent analog characteristics, which

have application to adjustable voltage and current sources, timing delay elements, RF matching, and a whole host of other analog and digital circuits [13]. This comes with outstanding device reliability; nonvolatile memories exceed industry norms of 100,000 rewrite cycles of endurance and 10-year retention times by wide margins. Furthermore, SAS is process-independent and has been proven in hundreds of circuits in many foundry processes over the past 10 years.

Architecture

The Zuma design consists of a complete communications transponder incorporating modem, local oscillator, power management, memory, and digital controller functions per the block diagram of Fig. 2. The properties of the air interface, including the modulation format of the forward and reverse links and power spectral densities, are illustrated in Fig. 3. Reader-to-tag signaling is via amplitude modulation of data encoded in the pulse width, but use of frequency shift keying (FSK) for tag-to-reader communication makes for an especially robust collision detection strategy and forgiving phase noise requirements in the reader. The bandwidth requirements, however, discourage use of the protocol outside of the United States.

Analog

Antenna Interface — A typical tag configuration consists of the Zuma chip flip-mounted on a printed antenna (paper or plastic label substrate) having 300 Ω terminal impedance, although we have built complete tags with a variety of antenna geometries, materials, and impedances. Power levels for startup and read operation are around –14 dBm, or 154 mVpeak from a 300 Ω source. The capacitive component of the rectifier input impedance can be resonated out by proper antenna tuning, giving a parallel equivalent source impedance of 650 Ω and peak voltages of 228 mV. Still, the sustainable DC output per diode is significantly less than the peak; design of the rectifier therefore starts by planning the DC gain per stage, which sets the number of stages for a given output voltage.

Rectifier (RECT) — The rectifier converts the incident RF signal energy to a direct current (DC) voltage to supply power for tag operation. The circuit is based on a Dickson charge pump, with the RF signal acting as the pumping clock. Supporting the main rectifier is a startup circuit that provides the bias current to the primary rectifier stack.

An ideal Dickson charge pump operates by shifting charge progressively up a diode stack. Often, such circuits require Schottky diodes to be available in the process to get acceptable performance at microwave frequencies, but these are not standard features of logic CMOS. We effectively work around the need for Schottky diodes by using MOS structures having a unique device design consistent with the layers in standard logic processes. Management of threshold voltages is a key requirement; these thresholds reduce the voltage multiplication of the charge pump and increase the minimum input voltage for operation. Our devices have their gates dynamically biased near the threshold in order to respond to small amplitude input signals; these bias voltages are indexed to process and temperature.

Modem (MOD and DEMOD) — Implementing the air interface requires demodulation of the forward link from the reader and modulation of the reverse link by changing the antenna impedance and therefore the tag's radar cross-section, allowing bidirectional transfer of digital data even though the reader supplies the only active source of RF power.

The demodulator serves to detect the AM waveform and output a digital representation of the envelope. The digital output pulses from the demodulator are passed to the controller logic, where symbol decisions are based on the relative widths of pulses. Since the forward link data is encoded into the duration of the AM, the demodulator must accurately recreate these pulse widths for digital symbol detection. Demodulation relies on conventional approaches involving peak and envelope detection, as well as a slicer.

Data timing is controlled by the duration of the reader data pulses and data calibration pulses. With regard to data timing, the salient feature of the demodulator is the output pulse duration and resolution as set by the circuit bandwidth and slew rate. The demodulator bandwidth must be sufficient to resolve the narrowest input pulse and the narrowest time interval between symbols, this being the dominant factor in bit error rate (BER) performance, but the modest currents permissible from the limited power budget require especially careful circuit design.

Oscillator (OSC) — The oscillator is the source of the system clock and the two FSK reverse link frequencies. Attached to the oscillator are two dynamic dividers (/2 and /3), used to generate the system clock and backscatter frequencies. After calibration, the nominal frequency is 6.6 MHz, leading to FSK frequencies of 2.2 and 3.3 MHz (logic 0 and 1, respectively).

The oscillator architecture is based on a source-coupled differential pair. Phase noise performance is very forgiving relative to use of local oscillators for heterodyning, needing frequency stability only within 1 percent, but variation over semiconductor process tolerances remains an issue. In this regard, SAS design techniques have application to consistent stable oscillator frequencies.

Power Management (PMU) — The power management block serves to provide regulated currents and voltages for other circuit blocks on the chip. For analog functions, this provides high power supply rejection in spite of the extreme variability in input power, but for the digital logic, regulation also helps ensure timing predictability.

In addition to supplying clean power, this block also senses when the chip is put into a reset condition (nominally, 850 μs of CW power) and detects when insufficient power exists for performing write operations.

Self-adaptive silicon design techniques allow electrically tunable transistors with permanent analog characteristics, which have application to adjustable voltage and current sources, timing delay elements, RF matching, and a whole host of other analog and digital circuits.

Digital functions performed by the chip consume the greatest power, requiring the use of circuit design styles that minimize switching energy, including operation in the subthreshold region of device bias.

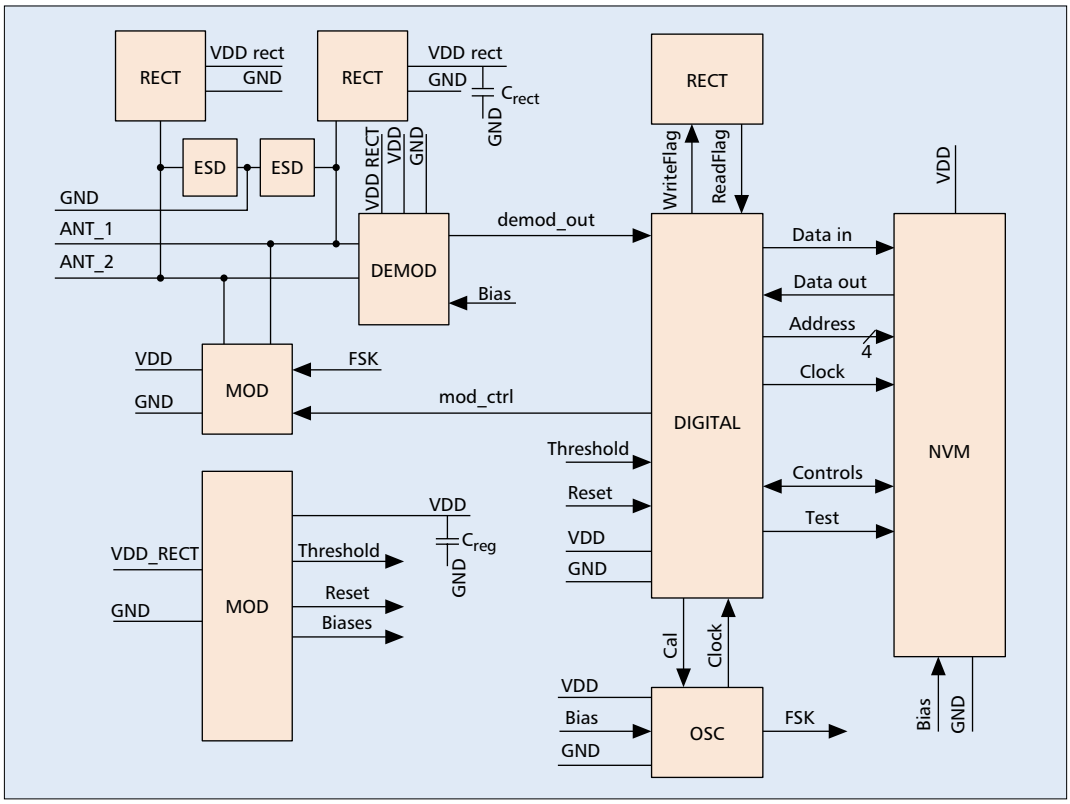

Figure 2. *The Zuma block diagram.*

DIGITAL

Digital functions performed by the chip consume the greatest power, requiring the use of circuit design styles that minimize switching energy. Operation in the subthreshold region is used to minimize the overlap current, important not only to prevent energy waste, but also to limit power supply spikes applied to the relatively high impedance power source. A specially designed cell library was created for the chip, inasmuch as conventional standard cell library elements impose too great a power and area penalty.

Digital functions are partitioned into circuits for the tag controller and a separate NVM controller that handles the rather sophisticated algorithm used to write to the memory.

Tag Controller (DIGITAL) — The tag controller performs numerous communication, calibration, and maintenance functions, including:

- Decode symbols received from the demodulator, and encode reverse link symbols provided to the modulator.
- Interpret a wide array of global and singulated (tag individually addressed) commands, 19 in all.
- Process commands and data symbols to advance through defined states and provide the necessary control signals.
- Implement cyclic redundancy checks (CRCs) to enhance air interface link reliability.
- Generate dynamic and static random numbers for an accelerated identification process.
- Interface to NVM to perform READ and WRITE operations.
- Implement security functions such as NVM lock-down and tag kill.
- Manage oscillator calibration and built-in test functions needed to exhaustively test and calibrate the chip following manufacture. Test support, while not fully self-contained, pays back the silicon area many times over in terms of overall manufacturing cost.

Events tend to occur either during power-up initialization (or a frequency hop) or in response to receiving a data symbol from the reader. During initialization, the reader transmits CW for a defined period, and the controller measures this time span with sufficient margin to cover oscillator frequency inaccuracy. At that time system reset is asserted, and the timing calibration block begins the calibration routine.

Once past the initialization sequence, the tag can process global commands or execute the singulation process whereby the reader identifies and communicates individually with any tags in its field. Data is transmitted from the reader one data symbol at a time, from an alphabet of three symbols (0, 1, null). The controller processes each symbol individually, such as when performing a binary tree traversal to singulate tags, or collects a series of symbols to process a command and any arguments and/or data associated with that command. Ten defined states exist within the protocol, with state machine outputs updated on a symbol-by-symbol basis. Figure 4 shows the state transitions and events defined in the Class 0 protocol.

MEMORY

The Zuma nonvolatile memory is formatted in a 256-bit block, plus configuration bits. It offers extremely low power (900 fJ/bit read, < 400 nA

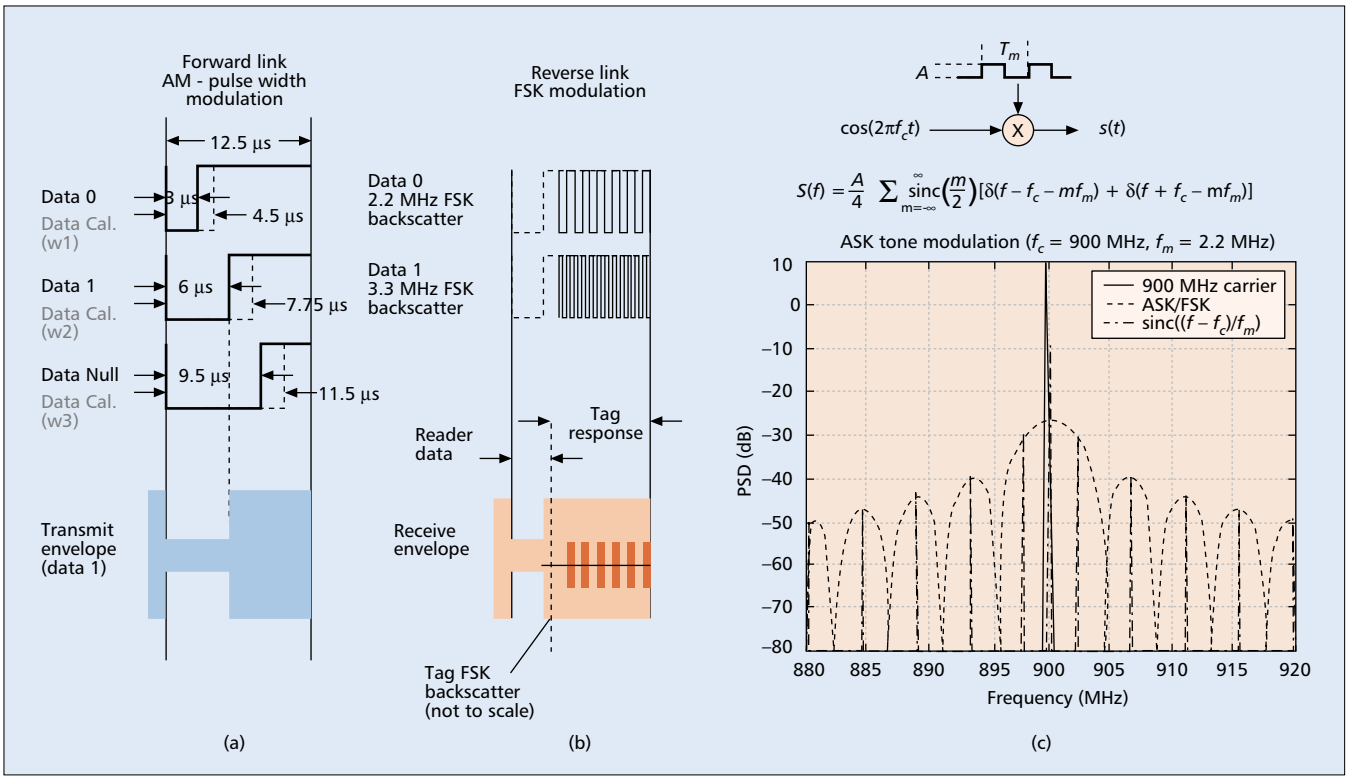

Figure 3. *Class 0 signal properties: a) forward link; b) reverse link; c) power spectral density.*

standby current), relatively fast write times (< 10 ms/row), 100,000 cycle write endurance (assumed uniformly distributed over the tag lifetime), and 10-year retention.

As with other applications of SAS technology, NVM circuits are able to store information by modifying the charge stored on floating-gate pFET transistors; the memory cell state is then read by measuring the current of these devices when power is applied. The use of pFET in lieu of nFET devices offers better retention, higher endurance, and no additional complexity within standard logic CMOS processes. The fact that these circuits can be implemented in standard logic processes represents a substantial advantage in multiple ways:

- The process requires the least number of total manufacturing steps (about 30 percent fewer relative to EEPROM) and is higher yielding.
- There is no compromise on using the process node (0.25 µm today) that offers the best value (wafer cost vs. die per wafer).
- The process is generic, available from multiple manufacturing sources.

The basic cell is depicted in Fig. 5. It is a differential cell with two floating gates, Fg_0 and Fg_1. By storing a different number of electrons it is possible to establish a voltage differential between the two gates. When the NVM cell is powered through terminal V, a difference in readout currents I_0 and I_1 is present and a sense-amplifier can consequently be used to discern the logic value stored in the cell. The condition $I_0 > I_1$ may be used to signify the logic zero, whereas the opposite condition can be used to denote a logic one. By applying the appropriate voltages to terminals V_{0c}, V_{0t}, V_{1c}, V_{1t}, and V, a sufficiently large electric field can be established across the oxide to allow Fowler-Nordheim tunneling to occur.

Layout

The completed chip layout is shown in Fig. 6, and includes 41,798 devices in a chip size of only 766 µm/side, distributed as follows:

nMOS	18,723
pMOS	20,328
Capacitor	2533
Resistor/diode	214

This is considerably more compact than other first-generation read-only tag chips, which vary from 925 µm /side to 950 µm /side, yet Zuma supports a much richer feature set, extended commands, read and write capability, and longer range. These benefits trace directly to the use of SAS circuit design techniques and careful optimized layout.

Performance

Measurements of the Zuma chip show typical read range performance of 11 m for read operations, with ultimate performance determined by the physical size and impedance characteristics of the antenna/label assembly. For writes, distances of 8 m are observed, exceeding the previous state of the art by wide margins, and delivering write ranges comparable to what other designs deliver in basic read-only performance.

Future Directions

RFID for the supply chain is in a developing state of maturity, and the industry now recognizes the opportunities that will be missed without a second-generation standard. We see the

evolution of RFID driven by lessons learned over the past two years, with a central role played by EPCglobal, a not-for-profit standards-driven organization that represents the needs and capabilities of end users and solution providers alike. Descended from the Uniform Code Council, the body that standardized bar code labels through the UPC, EPCglobal is bringing consistency to the use of EPCs in RFID labeling.

Below, we present our informed view of the factors driving RFID technology as it prepares for large-scale rollout in supply chain applications.

The "Top 10 List"

Open standards and interoperability: The industry has benefited from the role played by early adopters; however, large-scale deployment demands that users and suppliers come together to adopt one standard communication protocol. IEEE 802.11 standards activities serve as a model for this approach. Adoption rates are hampered by proprietary systems offered by single-source suppliers; to reach its full potential, the industry must recognize the need for a sufficient number of manufacturers of both tags and readers to meet demand. As a corollary, RFID technology must support scenarios where tags can be physically recognized by any legitimate user.

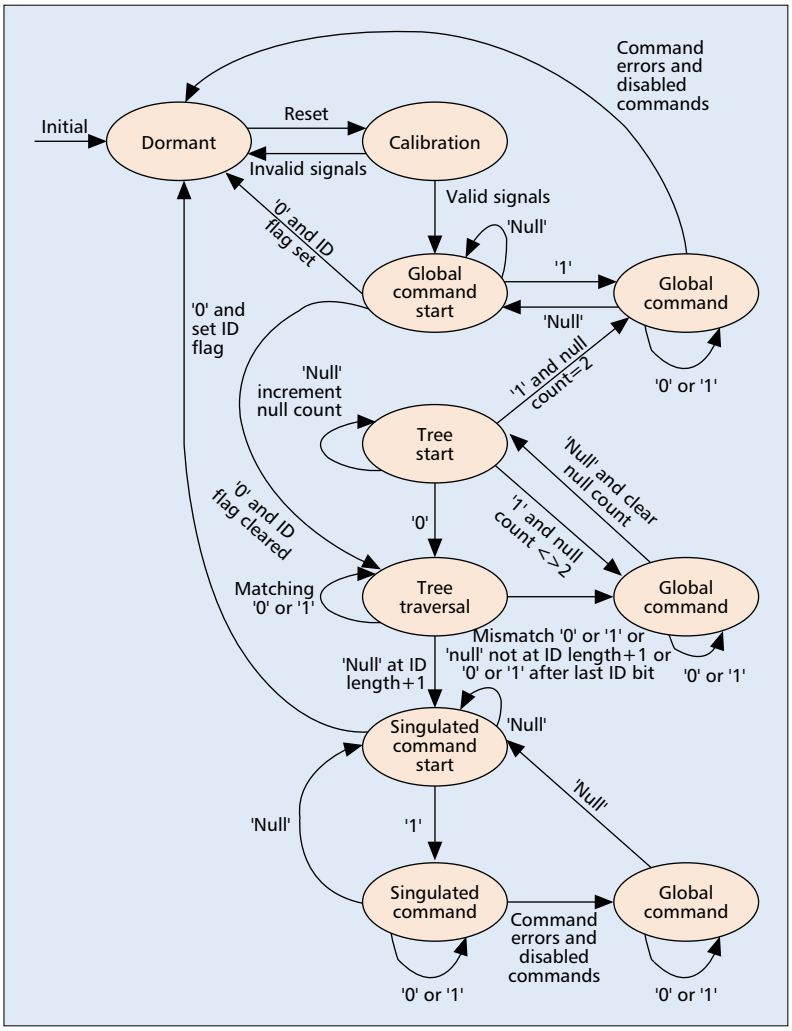

Figure 4. *Zuma (class 0 protocol) state diagram.*

Bulletproof operation: Field trials and pilots have shown promising but inconsistent performance, especially in harsh electromagnetic environments. System performance should be within at least 200 PPM of 100 percent reliable operation. This requirement calls for careful analysis of margins to ensure robust operation without such excessive over-design that costs get out of line with the tag's informational value.

Worldwide regulatory compliance: The protocol must be accepted globally with respect to any government's regulatory agency, and be configurable to exploit more liberal regulatory environments while avoiding power levels that would require a site license.

Aggressive cost reduction: Protocol and communication methods should function at levels that allow alternate and possibility cheaper tag antenna materials such as metallic ink to be used while still maintaining margin above minimum performance requirements. Costs should also come down in a Moore's law sense as semiconductor process technology advances.

Field writability and support for user data: Tags must be writable and lockable by intermediate and end users. The tag must be lockable so that EPC data cannot be changed once it has been written, and the protocol must also have an efficient verification mechanism to ensure the write was successful. The entire write cycle (write and verify) must be accomplished in tens of milliseconds per tag to allow for personalization at the item or carton manufacturing level; this speed is based on currently operating and forecast production lines.

Requirements flow down from actual use cases: Good engineering design dictates that requirements must be derived from identifiable needs in real applications. With an emphasis on supply chain uses, next-generation RFID systems now consider and analyze relevant scenarios, including:

- Single cases on conveyors at forecast production line speeds
- Pallet tags (including reusable asset tags, as well as disposable tags laced within the shrink wrap, similar to today's SSCC bar-code labels) driven through portal at maximum forklift speeds
- Case tags on loaded pallets in the presence of potentially overwhelming numbers of item tags
- Luggage tags on airport tugs traveling at high rates

In activities sponsored by EPCglobal, the metrics behind such scenarios have been identified across a broad range of users, and the results have significantly influenced protocol development.

Predictable performance: Most users require that tags be readable at greater than 5 m under controlled conditions, with write range of at least 1 m. Our present results show that this can easily be met, but reliable operation over these modest distances has not always been the case. Stories are told about how some manufacturers' tags even experience noticeable degradation after every read attempt.

Operation in dense reader environments: Readers and associated antennas (whether

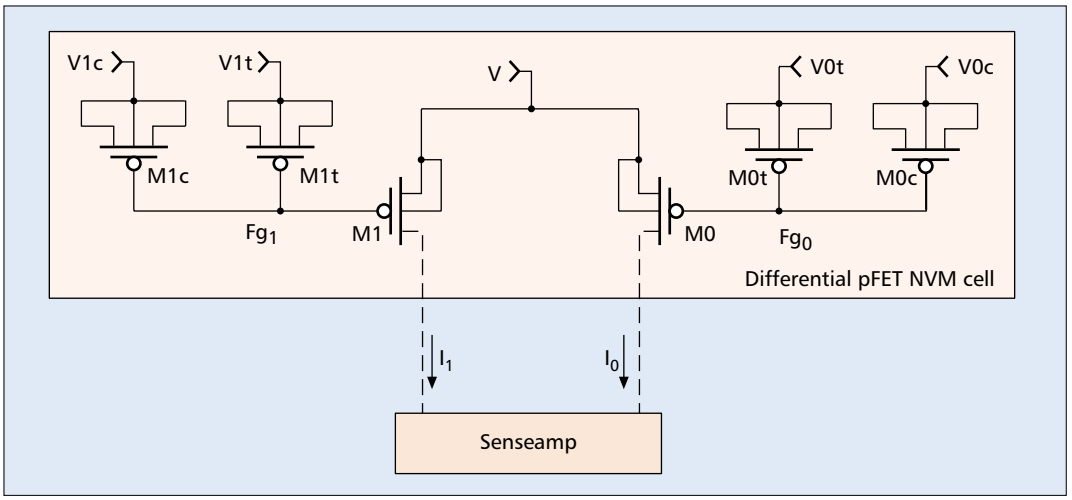

Figure 5. *The NVM circuit approach based on self-adaptive silicon.*

portable or fixed) should be able to function within close proximity without interference. Particularly in settings such as truck portals, where the dock door spacing leads to closely spaced readers, the potential for jamming is great.

Functionality that works cooperatively with database accesses: Tags must support bit masks to query for specific objects, to minimize RF traffic and torrents of redundant information that then has to be filtered out in software. This capability should allow inclusion or exclusion of tags by use of logical operations. When user data is provided, it should be possible to query tags on this field as an option to the unique EPC identifier.

Security and privacy: RFID systems must have a secure forward link to avoid eavesdropping. Encryption, while not needed for the vast majority of applications, may nonetheless be critical in some. Especially for consumer product uses, when individual items are tagged but ultimately leave the supply chain, tags must support a kill function that prevents the tag from responding in any way once disabled. This protects the identity of consumers that might otherwise be compromised by sophisticated data mining operations, addressing legitimate concerns raised by privacy advocates. Finally, specific applications will need the ability to put tags to sleep while the product is in transit, denying access to readers that lack a legitimate need to know. The ability to read (or even write or kill) is then bypassed until supplying the tag a predetermined password.

Technology Roadmap

An industry consortium of major RFID system, chip, tag, and reader suppliers has come together to advance a flexible standard extensible to higher tag classes [14]. Known as the Gen2 Protocol, this system incorporates the requirements listed above and, through the benefit of hindsight that comes from first implementations, does so at markedly improved range and tag throughput, and with smaller die area and power budgets while using only mature technologies. Figure 7 quantifies these benefits.

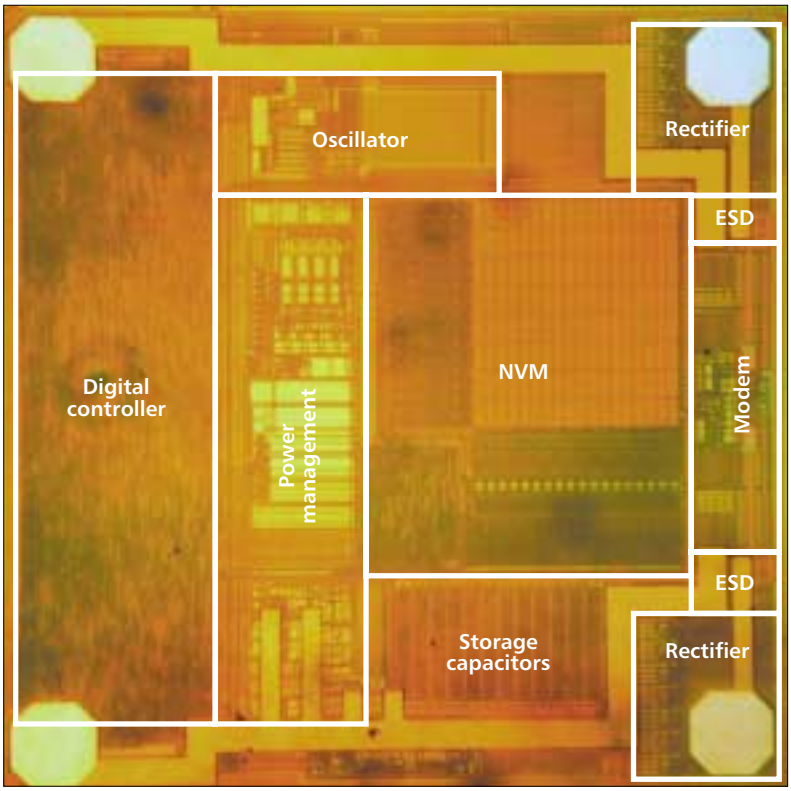

Figure 6. *The Zuma die layout.*

From implementation experience, we believe that the simplest digital CMOS will always be the process of choice, and the most cost-effective process will likely be two generations behind the "bleeding edge," where one finds mature process flows, stable yields, commodity processes from multiple suppliers, and proven reliability. We also believe that, while simplicity is desirable, cutting corners on digital functionality is unwise. As processes shrink, the digital circuits scale most aggressively, making them progressively cheaper with time.

With the advent of the Gen2 protocol, a high-value solution for a broad range of users has emerged [15]. RFID for supply chain applica-

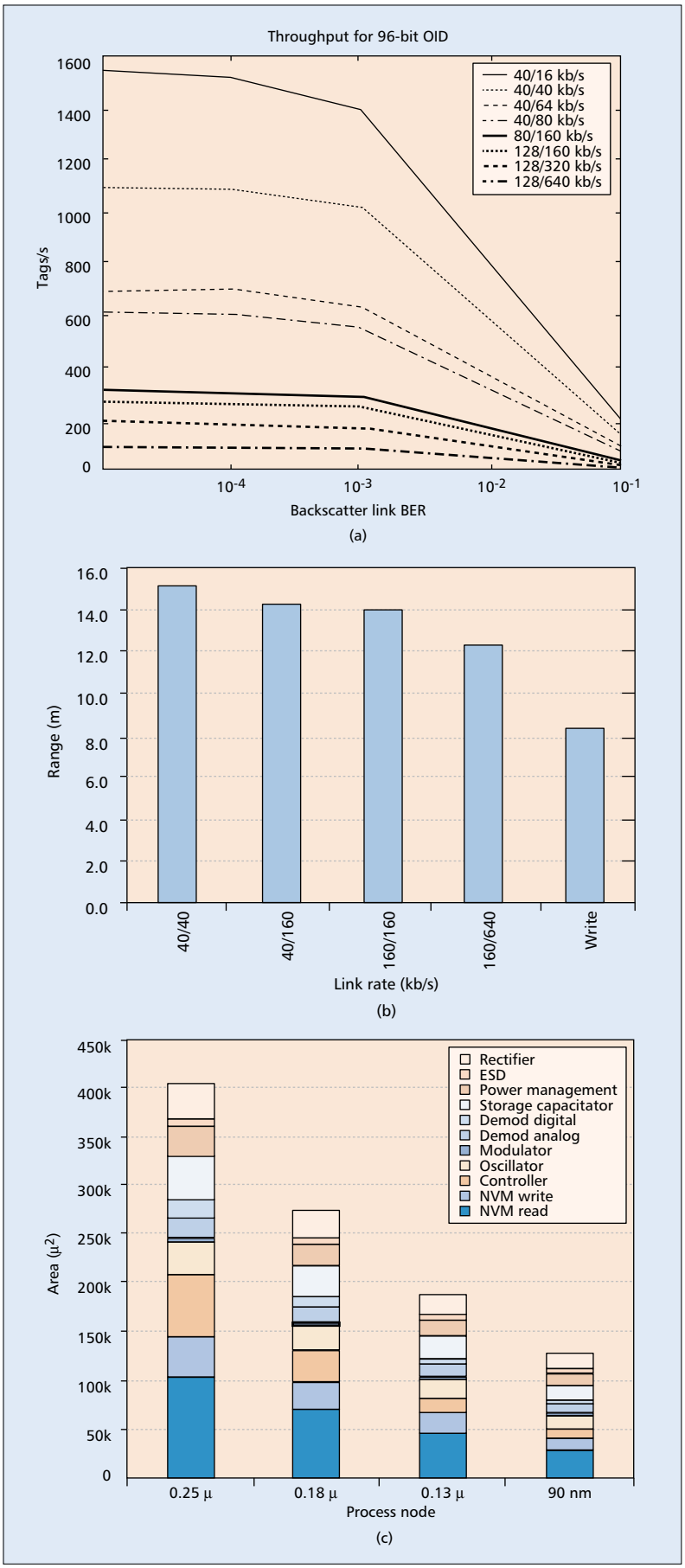

Figure 7. *Generation 2 RFID metrics: a) throughput; b) range; c) die size with process scaling*

tions is now poised to fulfill the promise advanced by its early proponents at MIT. Within the next few years, RFID will work into the supply chain mainstream, offering substantial economic benefit by directing the flow of goods worldwide in a mistake-proof, just-in-time manner.

Acknowledgments

The authors gratefully acknowledge the help and support of numerous individuals and companies in the user and solution provider community, working through EPCglobal to make RFID a commercial reality.

References

[1] PBI Media LLC, "Spelling Out the RFID Value Proposition," *Supply Chain Mgmt. Rev.*, Apr. 2004, http://www.manufacturing.net/scm/article/NEd0413000.2el?text=rfid
[2] MIT Auto-ID Center, "The Networked Physical World: Proposals for Engineering the Next Generation of Computing, Commerce, and Automatic Identification," MIT-AUTOID-WH-001, 2000, http://auto-id.mit.edu/research/whitepapers.html
[3] T. Scharfeld, "An Analysis of the Fundamental Constraints on Low Cost Passive Radio Frequency Identification System Design," M.S thesis, MIT, C.ambridge, MA, Aug. 2001.
[4] Case studies in applications of RFID: http://www.rfidjournal.com/article/archive/17
[5] S. Sarma, "Towards the 5¢ Tag," MIT Auto-ID Center, Nov. 1, 2001
[6] "860 MHz–930 MHz Class 0 Radio Frequency Identification Tag Protocol Specification Candidate Recommendation," v. 1.0.0, MIT Auto-ID Center, June 1, 2003
[7] C. Diorio, "Neurally Inspired Silicon Learning: From Synapse Transistors to Learning Arrays," Ph.D. dissertation, Caltech., Pasadena, CA, 1997.
[8] C. Diorio, D. Hsu, and M. Figueroa, "Adaptive CMOS: From Biological Inspiration to Systems-on-a-Chip," *Proc. IEEE*, vol. 90, no. 3, Mar. 2002.
[9] U.S. Patent 5,990,512, "Hole Impact Ionization Mechanism of Hot Electron Injection and Four-Terminal pFET Semiconductor Structure for Long-Term Learning," 1999
[10] U.S. Patent 5,898,613, "PMOS Analog EEPROM Cell," 1999.
[11] U.S. Patent 6,144,581, "PMOS EEPROM Non-Volatile Data Storage," 2000
[12] A. Pesavento *et al.*, "Adaptation of Current Signals with Floating Gate Circuits," *Analog ICs and Sig. Processing*, no. 30,pp. 137–47, Kluwer, 2002.
[13] M. Figueroa, D. Hsu, and C. Diorio, "A Mixed-Signal Approach to High Performance, Low Power Linear Filters," *IEEE J. Solid State Circuits*, vol. 36, no. 5, May 2001.
[14] Jupitermedia Corp., "Next-Generation RFID Standard Gathers Support," *Supply Chain Mgmt Rev.*, Apr. 2004; http://www.manufacturing.net/scm/article/NEi0420001.5cm?text=rfid
[15] EPCglobal, "EPC™ Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz," v. 1.0.0, Apr. 2004.

Biographies

Rob Glidden [S'75, M'78] (rob.glidden@impinj.com) is director of engineering at Impinj, Inc., responsible for RFID technology at both the Seattle, Washington and Newport Beach, California sites. He has been directly involved in development of analog, digital, and mixed-signal integrated circuit products for over 20 years in many bipolar, CMOS, and BiCMOS processes. Prior to joining Impinj, he was director of engineering at AMCC, responsible for all SiGe projects at three sites, generally focused on optical fiber communications chips at 10 and 40 Gb/s, and before that held design engineering and management positions for RF and other communications-oriented integrated circuits at TDK Semiconductor, Silicon Systems, and TRW. Early in his career, he was a Naval officer assigned to the Division of Naval Reactors, responsible for reactor plant electronics for the Trident submarine. He earned his B.S.E.E. degree from Cornell University in 1977 and his M.S.E.E. from the University of Southern California in 1978.

CAMERON BOCKORICK joined Impinj in September 2001, where he is currently senior layout designer. Prior to joining Impinj, he crafted high-performance mixed-signal layouts for Agere Systems and 3Com Silicon Technology Group. He earned his A.A.S. at Lehigh Carbon Community College in 1996.

SCOTT COOPER [M'90] received B.S. and M.S. degrees in electrical engineering from the University of Illinois, Urbana-Champaign in 1986 and 1988, respectively. He joined Impinj, Inc, Seattle, Washington, as lead system engineer in January 2001. Prior to joining Impinj, he worked as a senior staff engineer for TRW, Inc., Redondo Beach, California, and a staff engineer for Motorola, Libertyville, Illinois.

CHRIS DIORIO [M'88, S'93, M'97] is an associate professor of computer science and engineering at the University of Washington, and is a cofounder of Impinj, Inc., Seattle, Washington. He currently serves as a co-chair of the EPCglobal Hardware Action Group, tasked with developing next-generation RFID standards. He received a University of Washington Distinguished Teaching Award in 2001, an ONR Young Investigator Award in 2001, an Alfred P. Sloan Foundation Research Fellowship in 2000, a Presidential Early Career Award in Science and Engineering (PECASE) in 1999, a Packard Foundation Fellowship in 1998, and the Electron Devices Society's Paul Rappaport Award in 1996. He has worked as a senior staff engineer at TRW, Inc., senior staff scientist at American Systems Corp., and technical consultant at The Analytic Sciences Corp.. He received his B.A. in physics from Occidental College in 1983, and his M.S. and Ph.D. in electrical engineering from California Institute of Technology (Caltech) in 1984 and 1997, respectively.

DAVID DRESSLER received his B.S.E.E. degree from the University of Southern California, Los Angeles, in 1979, and his M.S.E.E. degree from West Coast University, Los Angeles, in 1986. He has been a board and IC designer for 25 years. He joined Impinj in 2000, initially concentrating on signal processing IC design and now focusing on ultra-low-power RFID digital IC design. Previous experience with TRW included IC, board, and unit level designs on multichannel demodulators for secure military satellite communications.

VADIM GUTNIK [M'00] earned a B.S. in electrical engineering and materials science from the University of California at Berkeley in 1994, and his S.M. and Ph.D. in electrical engineering from MIT in 1996 and 2000. Academic interests have included micromechanical resonators, variable-voltage power supplies, and high-speed low-skew clock distribution. From 2000 to 2003 he worked on SONET transceivers at Silicon Labs. He is currently an analog design engineer with Impinj.

CASEY HAGEN is a digital designer and earned his B.S. in computer engineering from the University of Washington in 2002.

DENNIS HARA [M'94] has over 20 years of experience in IC design. His early career experience was with Seattle Silicon Corporation, one of the first providers of standard cell layout and design analysis tools. Before Impinj, he spent time at NextComm, Inc., where he played a major role in the design of their 802.11 baseband processors, and at Zilog, Inc., where he managed a mixed-signal design group.

TERRY HASS [A'90] has 24 years of custom analog/digital IC design experience spanning a wide array of technologies including CMOS, bi-CMOS, silicon bipolar, and GaAs FET. Experience also includes designing, building, and testing of ICs, hybrids, modules, boards, and subsystems. He has acted as technical lead for specification definition, development of design guidelines, and architecture studies for numerous designs. He was twice nominated for and once awarded the prestigious TRW Chairman's Award For Innovation for work associated with developing the world's first spectrally efficient high data rate satellite modem.

TODD HUMES serves as chief technical officer for Impinj. His most recent positions were as product line manager for frequency synthesizers, and manager of the Frequency Synthesizer and Demodulator Department, both at TRW, Inc. He has developed a 12.8 Gb/s optical demodulator and bit synchronizer, a 5.5 GHz phase-locked loop (jointly with Dr. Diorio), and has managed numerous leading-edge technology programs. He earned his M.S. in electrical engineering from Caltech in 1989, and is a TRW Chairman's Award winner for innovation.

JOHN HYDE [M'95] received a B.S. degree in electrical engineering from the Massachusetts Institute of Technology, Cambridge, in 1972. He joined Impinj, Inc., in June 2000 as chief engineer. His design work at Impinj includes an RFID tag demodulator, a low-power logic CMOS NVM for RFID tag applications, and a logic CMOS 300-MS/s, 14-bit DAC using floating gate calibration. Prior to joining Impinj, he worked as a consultant, from 1978, and as an employee from 1972, at TRW, Inc. His design work at TRW included high-speed (400 Mb/s to > 10 Gb/s) digital and mixed-signal integrated circuits in silicon bipolar as well as GaAs and InP HBT, analog-to-digital converters, and frequency synthesizer circuits.

RON OLIVER received a B.S.E.E. degree from Virginia Polytechnic Institute (Virginia Tech) in 1994. His primary focus has been in the field of radio engineering. He worked for EVI Incorporated, Columbia, Maryland, designing hybrid microelectronic receivers and transmitters. In 1998 he went to Ericsson, Research Triangle Park, North Carolina, where he worked on CDMA cellular handset development. He joined Impinj in 2000 to develop high-performance RF circuits in standard CMOS based on self-adaptive silicon technology.

OMER ONEN received a B.S. degree in electrical engineering from the University of Victoria, British Columbia, Canada. He joined Impinj, Inc. in July 2002 as an RF design engineer. From 1999 to 2002, he worked for Electrobit, Inc., designing wireless local loop products. From 1998 to 1999 he designed a low-power ISM band transceiver product at ACR systems, Inc. He also designed satellite transceiver circuits while at Narrowband Telecom, Inc., from 1996 to 1998.

ALBERTO PESAVENTO received a Dr.Eng. degree in electrical engineering from the University of Padua, Italy, in 1995, and his M.S. and Ph.D. in electrical engineering from Caltech in 2001. While working toward his Ph.D. his main research interests were analog and mixed-signal VLSI, floating gate technology, and signal processing. He joined Impinj in 2001, and has led the development of several NVM memories in various CMOS logic processes. His interests are NVM technology and low-power low-voltage VLSI design.

KURT SUNDSTROM is a senior systems engineer at Impinj, Inc. He received a B.S.E.E. degree from Oregon State University in 1991 and an M.S.E.E. degree from the University of California at Davis in 1998. He has worked in the signal processing field for more than 10 years, including algorithm and hardware development for terrestrial microwave, satellite, DSL, wireless LAN, and RFID systems. His research interests include statistical and adaptive signal processing.

MIKE THOMAS received B.S. and M.S. degrees in electrical engineering from Virginia Tech, Blacksburg. He joined Impinj, Inc. in June 2000 as lead RF engineer. From 1996 to 2000 he worked for Allen Telecom, Inc., developing commercial cellular infrastructure products. He designed low-power wireless communications systems and circuits for government applications for EVI, Inc. from 1991 to 1996. From 1986 to 1991 he developed high-speed digital and analog-to-digital data acquisition systems and hardware for government customers at American Systems Corporation.

RFID for supply chain applications is now poised to fulfill the promise advanced by its early proponents at MIT. Within the next few years, RFID will work into the supply chain mainstream, offering substantial economic benefit by directing the flow of goods worldwide in a mistake-proof, just-in-time manner.