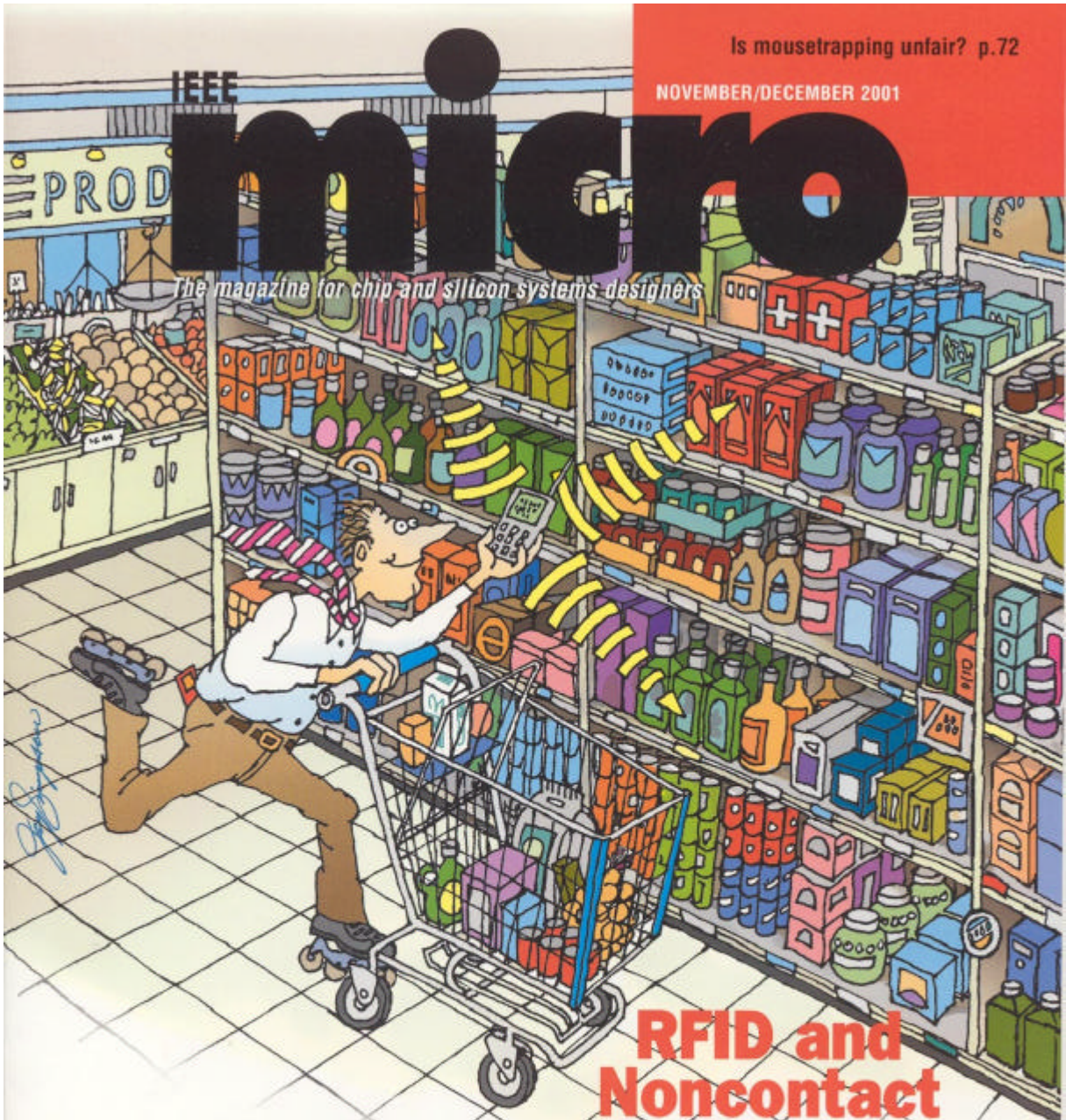


Is mousetrapping unfair? p.72

NOVEMBER/DECEMBER 2001

IEEE micro

The magazine for chip and silicon systems designers



<http://computer.org>

RFID and Noncontact Smart Cards

PLUS:
Efficient Software
Permutations

IEEE
COMPUTER
SOCIETY



Content

Special Features

- 4 **Guest Editor's Introduction: Radio Frequency Identification and Noncontact Smart Cards**
Ken Sakamura *University of Tokyo*
- 7 **The eTRON Wide-Area Distributed-System Architecture for E-Commerce**
The eTRON project addresses security issues related to RFID chip and smart card use.
Ken Sakamura and Noboru Koshizuka *University of Tokyo*
- 14 **Hardware and Software Symbiosis Helps Smart Card Evolution**
Chip and OS symbiosis make smart cards one of the smartest and least expensive of Security tokens.
Jean-François Dhem and Nathalie Feyt *Gemplus*
- 26 **Supplemental Cryptographic Hardware for Smart Cards**
Hardware functionality is necessary to meet smart card requirements not provided by software.
Elena Trichina, Marco Bucci and Domenico De Seta *Gemplus*
Raimondo Luzzi, University of Rome *La Sapienza*
- 36 **EasyRide: Active Transponders for a Fare Collection System**
Passengers with an EasyRide card can board public transportation vehicles without prior ticket purchase.
Thomas Gyger and Olivier Desjeux *EM Microelectronic Marin SA*
- 43 **An Ultra Small Individual Recognition Security Chip**
Hitachi mu-chips can aid inventory control of small objects and paper media.
Kazuo Takaragi, Mitsuo Usami, Ryo Imura, Rei Itsuki and Suneo Satoh *Hitachi*
- 50 **Radio Frequency Identification and the Electronic Product Code**
Inexpensive RFID systems could satisfy a wide range of commercial applications.
Sanjay Sarma, David Brock and Daniel Engels *MIT Auto-ID Center*

Features

- 56 **Efficient Permutation Instructions for Fast Software Cryptography**
Four new primitives make it possible to perform efficient, fast permutations in software. Such a capability accelerates cryptographic and multimedia processing.
RubyB. Lee, Zhijie Shi and Xiao Yang *Princeton University*
- 80 **Annual Index-Volume 21 Author and Subject Listings**

EASYRIDE: ACTIVE TRANSPONDERS FOR A FARE COLLECTION SYSTEM

THE EASYRIDE TICKETING SYSTEM RELIES ON RADIO FREQUENCY IDENTIFICATION CARDS OR TAGS TO MONITOR PASSENGER ACCESS TO PUBLIC TRANSPORTATION. CARDS EQUIPPED WITH A MINIATURE RADIO COMMUNICATION MODULE IDENTIFY PASSENGERS AND RECORD THE INFORMATION NECESSARY TO COLLECT FARES.

••••• Today's fare collection systems rely on a wide variety of paper tickets and on contact or contactless smart cards, which verify passengers using different means of public transportation. These distribution systems with intricate price lists and countless ticket offers have numerous shortcomings.

With one of the densest national public transportation networks in the world, Switzerland possesses a highly efficient system. Countless combinations exist for travel by train, ship, funicular, bus, and cableway. In this rich environment however, problems with ticket purchasing processes and customer information regarding the various price rate offers are far from being solved suitably. For this reason, the Schweizerische BundesBahn (SBB, or Swiss Federal Railways, the Verband Öffentlicher Verband (VöV, or Verband Public Transportation Association), which acts as a connecting link between most Swiss transportation companies, and Postbus—a country-wide regional public transport company—have joined efforts to define a global and innovative fare collection system called EasyRide.

EasyRide is a fare collection concept based

on active transponder technology. This allows efficient registration of passenger trips in place of inaccurate manual counting of passengers in the vehicles, giving transportation companies precise car occupancy statistics. This helps companies optimize their infrastructure with better vehicle distribution. Better use of vehicle resources enhances return on the operator's capital investment as well as heightens customer comfort with improved service.

Passengers equipped with an electronic card can board vehicles without prior ticket purchase. Equipment installed on each vehicle automatically detects the card and registers the passenger's entry and exit locations. The collected data—which contains the card and vehicle identification, stops names, and time stamps—is then forwarded from the vehicle to a fare calculation and billing system.

Passengers only need to carry the card in their pockets or luggage during the trip, and the whole access control process is executed unnoticeably.

In early 2000, after an initial project definition (see <http://www.easyride.ch>) and provider selection process, different industrial partners

Thomas Gyger
Olivier Desjeux
EM Microelectronic Marin
SA

began development and testing of the different parts (access control system, vehicle computer, back-end systems) of the entire system. The partners defined two field tests to demonstrate the EasyRide concept's feasibility and to experiment with the systems. The tests ran from February to May 2001 in Geneva and Basel. Each test involved approximately 30 equipped vehicles and 900 test customers, who traveled daily using their ticket card in different types of public transportation vehicles. The access control system was developed and installed in Geneva by the Swatch-EM Marin-Hayek consortium (<http://www.swatch.com>). Three types of vehicles were used: a suburban railway train, three and four door diesel buses, and cableways. In April 2001, the EasyRide project issued its first conclusions based on these field tests: The field tests proved the technical feasibility of the daily operational EasyRide system.

Operating method of the access control system

The EasyRide Access control system developed by the Swatch-EM Marin-Hayek consortium and installed at the Geneva test site takes into account the diversity of installation environments. The regional railway line between Geneva and La Plaine and run by the SBB can be categorized as suburban rail traffic in terms of speed of the trains and distances between the various stops.

Within the city of Geneva itself, on the other hand, on the Transports Publics Genevois (TPG, or Geneva Public Transport) lines, the number of buses in operation at any one time is much greater although the distances between the stops can be a question of meters.

In order to guarantee maximum reliability and optimum installation fees for each case, the access control system's operating method is adaptable to its usage environment. For this, it benefits from a technology derived from the keyless entry systems available on new generation automobiles.¹

System overview

Each public transportation user carries a card, which may also be called an active transponder. With this card, the user can get

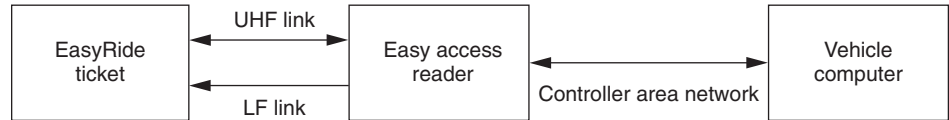


Figure 1. EasyRide Access system.

in and out of transportation vehicles equipped with the EasyRide Access system, without even pulling his card out of his pocket, suitcase, or handbag.

The main advantage of active transponders is the ability to communicate over a long distance at high data rates, as compared to passive transponders. The main difference between the active and the passive transponder is the power activation, that is, with or without a battery. Obviously, the drawback stands in the active part of the tag, which implies the use of a dry-cell-type battery. This drawback can be bypassed if the circuit is designed in such a way that the battery life duration exceeds the tag's lifetime, ensuring a reliable communication link.

The system's low-frequency (LF) field is precisely located near the vehicle entrances in a very well defined pattern. This LF field activates only the tags entering the defined area. The ultra-high frequency (UHF) field is unsuited for this use because of the difficulty of predicting its precise radiation pattern in closed or partly closed areas. In our figures, we represent the UHF field by a large homogeneous pattern, which in a real situation is absolutely not the case. Typically, the LF field is in the 125-KHz range, and the UHF in the 434 MHz.

Once the tag detects the LF input or output in the defined area, it starts to communicate with the system using the UHF link. The tag can then store in memory the date, time, and location of where the passenger came in and out. On the other hand, the access reader stores the tag's identification with other data specific to the tag, such as the card's identification.

Presence detection: BIBO mode

In BIBO mode (be in, be out), the system can detect the presence of all EasyRide cardholders between any two stops. These passengers' journeys are then recreated by back office software—a discussion of which is out of the range of this article—in terms of the stages on the bus line during which their pres-

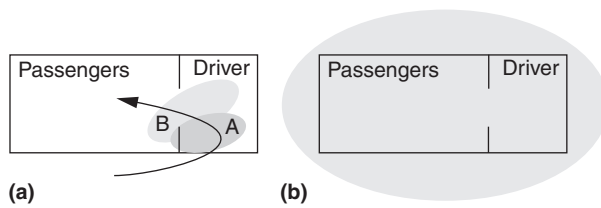


Figure 2. BIBO description. The two small ellipsoidal shapes, A and B, describe the LF fields that activate when a vehicle is stopped (a). The larger ellipsoidal shape covering the whole vehicle describes the UHF range, activated during the journey (b).

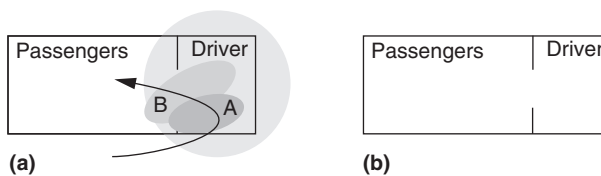


Figure 3. WIWO description. The two small ellipsoidal shapes, A and B, describe the LF fields; activate when a vehicle is stopped (a). The larger ellipsoidal shape covering the whole vehicle describes the UHF range, activated just after the card leaves the LF fields. The duration of UHF activation is only a few hundred milliseconds, the time it takes to exchange data between the card and vehicle (b).

ence was confirmed. The system's BIBO mode is ideal for an interurban environment.

When outside the vehicle, the EasyRide card stays in standby mode. A passenger entering a stationary vehicle will pass through two zones, A and B, as shown in Figure 2. These two LF fields both activate the card and send it telemetry data specific to the vehicle. Once activated, the card communicates with the access control system via radio signals sent at regular intervals during the journey, and acknowledged by the reader. The system can therefore monitor the presence of the passenger throughout the vehicle and for the entire duration of the journey. When the passenger leaves the vehicle, the card fails to receive acknowledges from the reader, so it returns to standby mode.

The BIBO mode is a simple concept. The presence of LF fields A and B at the vehicle entrance is not mandatory in basic BIBO mode. In the implementation made by EM Microelectronic Marin SA, these two fields enable discrimination between cards carried on a person who is passing nearby the vehicle

door without fully entering and on people that actually enter the vehicle; the card needs to receive information from both A and B fields to activate into BIBO mode.

Entrance/exit detection: WIWO mode

In WIWO mode (walk in, walk out), the system detects entrance and exit movements of all EasyRide cardholders. These passengers' journeys are then recreated by the onboard computer by using the stop at which they entered the vehicle and the stop at which they exited the vehicle.

As Figure 3 shows, a passenger entering or exiting a stationary vehicle will pass through zones A and B, which will activate the card out of standby mode and send specific data from the reader to the card. The order in which the card detects zones, that is, A then B or B then A, indicates whether the passenger is entering or exiting the vehicle. Once activated, the card communicates instantly with the access control system via a radio signal sent indicating whether it has been brought into or taken out of the vehicle. Once the reader has received the card's transaction information, it sends an acknowledge response signal, and the card returns to standby mode. WIWO mode is the most power effective, but cannot be installed on all the different kind of transportation platforms.

WIWO versus BIBO mode

WIWO and BIBO mode have different advantages and drawbacks. The Table 1 summarizes the main differences.

The main advantage of the WIWO mode lies in its exception handling of various *crooked* situations, such as a passenger getting in to help carry a luggage, but getting out at the same stop. In this case, and with the WIWO, the card has the intelligence not to generate a UHF telemetry link. This feature is only possible because the A and B fields are different, and because of the position of these two fields within the environment.

The main advantage of the BIBO mode lies in its possible simpler installation, and a more error-tolerant communication protocol. To simplify installation, if required, only one set of antennae for the LF field could be used, although this cancels the possibility of direction detection.

Table 1. Comparison of BIBO and WIWO modes.

Mode	Method	Advantage	Disadvantage	Ideal application
BIBO	Periodic polling of card data during the journey	Simple algorithm	Nonoptimized power consumption	Interurban environment, such as regional or long-distance trains
WIWO	Data transmitted just after entering or exiting the vehicle	Low power consumption	Heavy infrastructure Algorithm needs to handle more error cases	Intraurban environment with short distances between stops

Access control system components

The access control system is made up of readers placed near doors of public transportation vehicles. Each reader has antennae integrated with the vehicle infrastructure and which are used for the communication that takes place between the reader and the card issued to the passenger. The readers thus collect information contained within each card and transfer this data to the onboard computer via a controller area network (CAN) bus. The onboard computer then transfers the data to a central system via the Global System for Mobile Communications (GSM) radio network.

EM Microelectronic Marin SA's involvement in the EasyRide project involved the parts concerning access, that is, the card, the readers, and antennae.

Card

EasyRide cards, an example of which is shown in Figure 5, are the access key to the overall system. The cards have a miniature radio communication module and link the passenger and the access control system. The only condition for the use of these cards is that passengers must carry them on their person or in their luggage when traveling. The system automatically detects the cards, with no need for the holder to take the card out her pocket and pass it through or in front of a specific machine. The intelligence placed inside the card enables it to use both BIBO and WIWO modes simultaneously.

The EasyRide card was created using electronic components specially designed for the EasyRide project and guaranteeing minimum energy consumption. The card, which has the potential for further capacity extension, can currently retain up to 200 individual journeys,

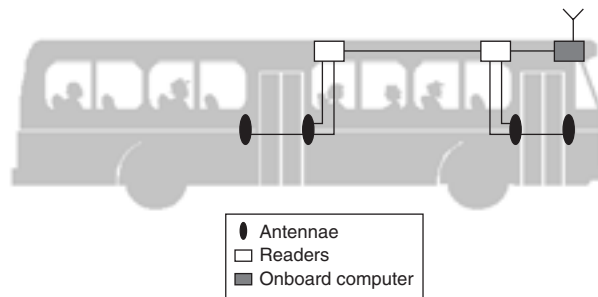


Figure 4. EasyRide Access installation.



Figure 5. EasyRide card used in the pilot test.

as requested by the EasyRide specification. This amount of data stored should be enough to match the card data with the individual's detailed bill. We expect that the card's lifetime will be over two years for an average passenger, as requested by the EasyRide specification.

Autonomy compliance is ensured by the sleep mode feature, during which very low power is required to listen for activate signal. This current, in the order of magnitude of just a few microamperes, drives a LF receiver that always listens for a specific header. Once the

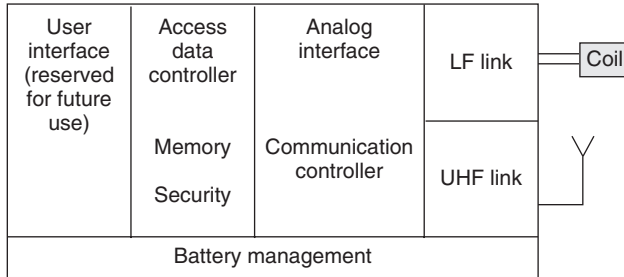


Figure 6. EasyRide card block diagram.



Figure 7. EasyRide reader installed inside a compartment.



Figure 8. EasyRide reader and a card.

header detected, the rest of the circuit is triggered and powered up, enabling long-range communication. This very low consumption target, with a high frequency receiver, could only be achieved using very low duty cycle listen time over sleep mode.

A 3-V lithium manganese battery with a

very low self-discharge rate powers the card. Figure 6 shows the card's structure.

A low-power, 4-bit microcontroller manages the whole card: Eeprom storage, LF receiver, and UHF transceiver. The microcontroller is a standard product clocked at 600 KHz, whereas, the LF receiver is a specific CMOS low-power, low-voltage design.

The UHF transceiver is also a very low-power design, in the milliampers range. However, as over 90 percent of the global power budget is used in standby mode by the microcontroller and the LF receiver, this design's overall consumption is in the microampere range.

The card's two antennae are housed in the same enclosure. An LF coil operates in a close coupling field (magnetic), and a UHF semi-loop operates in a coupled field. The cards are 0.2 inches thick, their overall dimensions are $85 \times 53 \times 5$ mm, about the size of a credit card.

Reader

The reader is an electronic device installed near the entrance doors to the public transportation vehicles. It is linked up to the onboard computer, which transmits to the reader the geographical position of the vehicle. The reader communicates with all cards within its operating range via antennae. It communicates to the cards the vehicle's position and identity. The reader reads the identification information on the cards..

The reader also communicates with the onboard computer, to which it sends the data it has received. The processing power of the reader manages the LF transmitter and the UHF transceiver.

The reader is of modest size and can easily be housed within one of the service compartments available on the various types of public transportation vehicles, as Figure 7 shows. The reader's dimensions are approximately $9.4 \times 7.1 \times 2.3$ inches ($24 \times 18 \times 6$ cm). Figure 8 shows a typical reader.

Antennae

The access control system uses two types of antennae: low frequency and high frequency.

LF antennae. These serve two purposes. Due to a patented 3D polarization, they activate any cards that pass into their operating range and can detect whether a passenger is entering

or exiting the vehicle. Their transmission frequency is 125 kHz and they guarantee the one-way communication from the reader to the card. They can be produced in various shapes and sizes for ease of integration into different vehicle types. Figure 9 shows a conical version, which is ideal for mounting onto bars or tubes, and a flat version suitable for mounting onto walls or partitions, as well as a card. Figure 10 shows a conical LF antenna installed on a vehicle.

UHF antennae. These antennae are used for bidirectional data communication, that is, between the card and the reader, during journeys. UHF antennae operate at a frequency of 433 MHz. They are made according to a slim design and can be easily mounted to ceilings or behind insulation partitions.

The EasyRide project was a technical challenge in many different ways. On the user side, in many public transportation vehicles, such as a metropolitan bus, there is no gate to restrict access in case the transportation ticket (card) is not valid. This means that the systems reliability of detection should be close to 100 percent or else the operator will lose money. This requirement along with the two year needed life powered by a single 3-V lithium coin battery, led us to a low-power, low-voltage receiver specification and implementation.

This active transponder concept opens the way to promising new applications linked to people flux, or item flux management. Micropositioning is another application for the EasyRide system technology. Although cellular phones using GPS provide excellent outdoor positioning information, indoor positioning is still under investigation. EasyRide applied to closed environments can address micropositioning issues.

Research trends based on this technology is toward a user interface on the card, and also having a thinner card. Our research labs are working on a thinner card, which basically implies a reduction in battery size, and hence a global power reduction of the overall card electronics. The techniques we are using to achieve these targets are basic principles such as global integration of all functions on a single chip, foundry process reduction, and antenna miniaturization, not to mention over-



Figure 9. Two LF antennae and a card.



Figure 10. LF antenna mounted on a pole.

Further resources

- EM4102 datasheet, EM Microelectronic Marin SA, 2000; <http://www.emmicroelectronic.com>.
- *EasyRide Concept*, EasyRide, Hirschengraben 2, CH-3011 Bern, Switzerland, April 2000 (in German or French).
- *Report on Urban Transport*, EasyRide, Hirschengraben 2, CH-3011 Bern, Switzerland, (in German or French).
- *Project UR1 Report*, EasyRide, Hirschengraben 2, CH-3011 Bern, Switzerland, April 2000 (in German or French).
- *Using Low Power Transponders and Tags for RFID Applications*, application note, EM Microelectronic Marin SA, Switzerland, 1999; <http://www.emmicroelectronic.com>.
- *RFID Made Easy*, application note, EM Microelectronic Marin SA, Switzerland, 1999; <http://www.emmicroelectronic.com>.
- EM6640 datasheet, EM Microelectronic Marin SA, Switzerland, 1999; <http://www.emmicroelectronic.com>.

all software optimization for a more efficient use of the available airtime.

MICRO

Acknowledgment

All of the companies within the Swatch-EM Microelectronic Marin-Hayek Engineering consortium were actively involved in the many phases of the EasyRide project.

Thomas Gyger is project manager for systems development in the Internet and high-tech business development team at Swatch Group, EM Microelectronic-Marin SA. His research interests include systems engineering with a focus on software development and data security. Gyger has an Ecole Technique Supérieure (ETS) degree in engineering from the engineering school of Saint-Imier, Switzerland. He is a member of the Swiss Informaticians Society.

Olivier Desjeux is project manager and group leader of RFID solutions support at EM Microelectronic-Marin SA. His research interests include radio frequency development with an emphasis on radio localization. Desjeux has a Diplôme d'Ingénieur in electrical engineering from the Ecole Française d'Electronique et d'Informatique, Paris and an MS in project management and quality from the Institut de Gestion Sociale. He is a member of the IEEE.

Direct question and comments about this article to authors, EM Microelectronic Marin SA, rue des Sors 3, CH-2074 Marin, Switzerland; tyger@emmicroelectronic.com or odesjeux@emmicroelectronic.com.