Review of the book

”RFID Design Fundamentals and Applications”

by Albert Lozano-Nieto

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-1-4200-9125-0

Jorge Nakahara Jr

June 2011

1 Summary of the review

The widespread interest for the technology surrounding the initials RFID (acronym for Radio Frequency IDentification) is responsible for a myriad of publications on this subject.
The introductory chapter is straightforward and accessible to everyone. But further chapters quickly become very technical, which makes it aimed at professionals with a strong background in eletronics, such as electrical engineers and (under)graduate students, since it provides a pletora of technical details that very likely these professionals could understand and profit from. It is also an interesting reference to compare RFID systems from different manufacturers, although there may be many and the listing is not exhaustive. Since it is a technology under development, we shall expect changes without notice concerning these devices and the protocols inside them. Nonetheless, this book provides a snapshot of the internal components and the communication (via radio signals) between the devices that will probably substitute the traditional bar codes in the near future.

2 Summary of the book

As the title of the book indicates, the contents emphasize design criteria of RFID systems for different applications. This book has eight chapters. In chapter one, the author starts by quickly defining the main components of RFID systems, including a transponder, an interrogator, a host computer and a database server. A transponder is typically called ”RFID tag” or just ”tag”, but contains an antenna, a chip and eventually some circuitry for storage and quick computation. The interrogator, also called ”reader”, consists of a device to read (and power) the transponder remotely via radio waves. A host computer is connected to one or more interrogators since the former has more powerful resources for more extensive computations. The database is used to store information about the transponders’ status and contents.
Chapter two deals with antennas for the RFID transponders. Details include the design (shape and size), electrical parameters such as inductance, impedance and resistance for different kinds of radio frequency: LF (low frequency), HF (high) and UHF (ultra high).
Chapter three details the internal circuitry of a transponder, electrical parameters, and its mains functional components: memory blocks, radio-frequency and power control structure, error control coding and anti-collision treatment.
Chapter four focus on antennas for interrogators, describing design decisions concerning radio frequency (LF, HF and UHF), electrical parameters (impedance, inductance), design and construction materials.
Chapter five describes interrogators. They have two basic functions: to generate and transmit the radio frequency signal used to energize the transponders and to receive and decode the backscattered signal generated by the transponders. In this chapter, the main building blocks of an interrogator are analysed: the tuning circuits, the modulator/demodulator, the power and signal amplifiers.

Chapter six describes the protocol used between interrogators during their communication. Examples are provided for interrogators manufactured by Texas Instruments (TI). These examples show basic communication protocols between interrogators and their host computers as a stepping-stone to understand the control of interrogators from other manufacturers. An example is the TIRIS bus protocol developed by TI.
Chapter seven explains the communication methods used to transfer information from an interrogator to a transponder (called forward communication link) or vice-versa (called return link). This chapter describes in detail different protocols used for systems operating the LF, HF or UHF ranges. An interesting protocol is for anticollision, when an interrogator sends a radio signal that reaches several transponders at the same time. Since each transponder will answer independently, the air will be saturated with radio waves from all of them transmiting back simultaneously, leading to several signal collisions at the interrogator. This event requires a protocol to identify one or a set of transponders as recipients of the original signal sent by the interrogator. This is the task of an anticollision protocol.
Chapter eight explores the structure and configuration of commands for transponders as well as the different status and error messages transmitted by the transponders as response to these commands. In particular, we note here the first reference to ISO/IEC 15963-3 and ISO 14443 protocols. Although a number of protocols and devices from different manufacturers were displayed, it was not clear that many of them were standardized, which may be due to the fact that RFID technology is rapidly changing.

3 What is the book like (style)?

The book starts with a quick introduction for the novice, explaining the basic components of an RFID systems, how they function and interact with each other. It is interesting to note that RFID technology is not new. It is mentioned that similar tags using radio waves were already used for detecting (that is, authenticating) friend or foo in World War II. Modern applications include its mass-scale deployment by the US Department of Defense in 2005 to facilitate its logistics, and by Wal-Mart for efficient logistical purposes, as well.
This book is divided into eight chapters. After the first chapter, though, the book starts to delve deep into technical details that are more suitable for eletronics engineers and (under)graduate students in related fields (see Sect. 2). The style is increasingly technical, almost like a brochure from a chip manufacturer, with plenty of minute electrical details of an RFID tag circuitry and the protocols used by these devices to communicate between them. The book provides plenty of pictures, formulas, graphs and schematics of circuits, and discusses extensively on design decisions, protocols and trade-offs depending on the particular application of the RFID tag, be it to track down pallets of goods, cattle and other animals, goods in a supermarket, immobilizers for cars and so on.
This book illustrates the design of commercially available products, and is helpful to people interested in knowing how such devices are programmed and how communication is performed remotely via radio signals.

4 Would you recommend this book?

The author already mentions that his book is aimed at ”professionals and students in electronics, telecommunications and new technologies”. I agree. The contents are truly aimed to electrical engineers and professionals who can better profit from the myriad of technical details that are mostly relevant for people wishing to implement, design, analyse or maintain RFID systems from an engineering perspective. This book is fully illustrated, with minute details of circuits, chips, schematic diagrams, and formulas for the voltage, inductance, and a summary of other parameters. Listing is not exhaustive, and the RFID systems mentioned are from commercial manufacturers such as Alien Technology, Atmel, Texas Instruments and Microchip Technology.
The absence of cryptographic capability in the RFID tags described in this book is a pity. At most, it describes the storage of passphrases in some parts of the tags, but there is no mention of cryptographic algorithms, neither symmetric nor asymmetric, that could be stored in the tags or in the interrogators. Also, the protocols discussed in this book are for low-level communication, not cryptographic protocols at all. Maybe the reason is that the storage and computational cost are mostly significant for low-cost

RFID tags (and also the lack of widespread standardization of both tags and algorithm that could fit in this resource-limited hardware).

Because of the amount of details of the circuitry and electrical parameters related to the internal components of the RFID tags, I would recommend this book to people working on side-channel analysis. Curiously, there is no mention of such attacks in the book, not even in the bibliography. Taking into account the lack of cryptographic algorithms themselves, it is no surprise. The aim of the author is to describe RFID systems in general, showing trade-offs depending on the cost and the application environment other than to provide clues for cryptanalysis. But, the possibility exists, and it is an idea for yet another book dedicated to these types of attack, when the technology advance to such a point that adding cryptographic algorithms will not be hindered due to scarce power and space in silicon.

The reviewer is an independent researcher.