INTRODUCTION

Radio Frequency Identification (RFID) systems use radio frequency to identify, locate and track people, assets, and animals. Passive RFID systems are composed of three components – an interrogator (reader), a passive tag, and a host computer. The tag is composed of an antenna coil and a silicon chip that includes basic modulation circuitry and non-volatile memory. The tag is energized by a time-varying electromagnetic radio frequency (RF) wave that is transmitted by the reader. This RF signal is called a carrier signal. When the RF field passes through an antenna coil, there is an AC voltage generated across the coil. This voltage is rectified to supply power to the tag. The information stored in the tag is transmitted back to the reader. This is often called backscattering. By detecting the backscattering signal, the information stored in the tag can be fully identified.

DEFINITIONS

Reader

Usually a microcontroller-based unit with a wound output coil, peak detector hardware, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation.

Tag

An RFID device incorporating a silicon memory chip (usually with on-board rectification bridge and other RF front-end devices), a wound or printed input/output coil, and (at lower frequencies) a tuning capacitor.

Carrier

A Radio Frequency (RF) sine wave generated by the reader to transmit energy to the tag and retrieve data from the tag. In these examples the ISO frequencies of 125 kHz and 13.56 MHz are assumed; higher frequencies are used for RFID tagging, but the communication methods are somewhat different. 2.45 GHz, for example, uses a true RF link. 125 kHz and 13.56 MHz, utilize transformer-type electromagnetic coupling.

Modulation

Periodic fluctuations in the amplitude of the carrier used to transmit data back from the tag to the reader. Systems incorporating passive RFID tags operate in ways that may seem unusual to anyone who already understands RF or microwave systems. There is only one transmitter – the passive tag is not a transmitter or transponder in the purest definition of the term, yet bidirectional communication is taking place. The RF field generated by a tag reader (the energy transmitter) has three purposes:

1. **Induce enough power into the tag coil to energize the tag.** Passive tags have no battery or other power source; they must derive all power for operation from the reader field. 125 kHz and 13.56 MHz tag designs must operate over a vast dynamic range of carrier input, from the very near field (in the range of 200 VPP) to the maximum read distance (in the range of 5 VPP).

2. **Provide a synchronized clock source to the tag.** Many RFID tags divide the carrier frequency down to generate an on-board clock for state machines, counters, etc., and to derive the data transmission bit rate for data returned to the reader. Some tags, however, employ on-board oscillators for clock generation.

3. **Act as a carrier for return data from the tag.** Backscatter modulation requires the reader to peak-detect the tag’s modulation of the reader’s own carrier. See page 2 for additional information on backscatter modulation.
SYSTEM HANDSHAKE

Typical handshake of a tag and reader is as follows:

1. The reader continuously generates an RF carrier sine wave, watching always for modulation to occur. Detected modulation of the field would indicate the presence of a tag.

2. A tag enters the RF field generated by the reader. Once the tag has received sufficient energy to operate correctly, it divides down the carrier and begins clocking its data to an output transistor, which is normally connected across the coil inputs.

3. The tag's output transistor shunts the coil, sequentially corresponding to the data which is being clocked out of the memory array.

4. Shunting the coil causes a momentary fluctuation (dampening) of the carrier wave, which is seen as a slight change in amplitude of the carrier.

5. The reader peak-detects the amplitude-modulated data and processes the resulting bitstream according to the encoding and data modulation methods used.

BACKSCATTER MODULATION

This terminology refers to the communication method used by a passive RFID tag to send data back to the reader. By repeatedly shunting the tag coil through a transistor, the tag can cause slight fluctuations in the reader's RF carrier amplitude. The RF link behaves essentially as a transformer; as the secondary winding (tag coil) is momentarily shunted, the primary winding (reader coil) experiences a momentary voltage drop. The reader must peak-detect this data at about 60 dB down (about 100 mV riding on a 100V sine wave) as shown in Figure 1.

This amplitude-modulation loading of the reader's transmitted field provides a communication path back to the reader. The data bits can then be encoded or further modulated in a number of ways.

FIGURE 1: AMPLITUDE – MODULATED BACKSCATTERING SIGNAL
DATA ENCODING

Data encoding refers to processing or altering the data bitstream in-between the time it is retrieved from the RFID chip's data array and its transmission back to the reader. The various encoding algorithms affect error recovery, cost of implementation, bandwidth, synchronization capability, and other aspects of the system design. Entire textbooks are written on the subject, but there are several popular methods used in RFID tagging today:

1. **NRZ (Non-Return to Zero) Direct.** In this method no data encoding is done at all; the 1’s and 0’s are clocked from the data array directly to the output transistor. A low in the peak-detected modulation is a ‘0’ and a high is a ‘1’.

2. **Differential Biphase.** Several different forms of differential biphase are used, but in general the bitstream being clocked out of the data array is modified so that a transition always occurs on every clock edge, and 1’s and 0’s are distinguished by the transitions within the middle of the clock period. This method is used to embed clocking information to help synchronize the reader to the bitstream; and because it always has a transition at a clock edge, it inherently provides some error correction capability. Any clock edge that does not contain a transition in the data stream is in error and can be used to reconstruct the data.

3. **Biphase_L (Manchester).** This is a variation of biphase encoding in which there is not always a transition at the clock edge.

**FIGURE 2: VARIOUS DATA CODING WAVEFORMS**

<table>
<thead>
<tr>
<th>SIGNAL</th>
<th>WAVEFORM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td><img src="image" alt="Digital Data Waveform" /></td>
<td>Digital Data</td>
</tr>
<tr>
<td>Bit Rate CLK</td>
<td><img src="image" alt="Clock Signal Waveform" /></td>
<td>Non-Return to Zero – Level</td>
</tr>
<tr>
<td>NRZ_L</td>
<td><img src="image" alt="Biphase – Level (Split Phase) Waveform" /></td>
<td>Biphase – Level (Split Phase)</td>
</tr>
<tr>
<td>Biphase_L</td>
<td><img src="image" alt="Biphase – Level (Manchester) Waveform" /></td>
<td>Biphase – Level (Manchester)</td>
</tr>
<tr>
<td>Differential</td>
<td><img src="image" alt="Differential Biphase – Space Waveform" /></td>
<td>Differential Biphase – Space</td>
</tr>
<tr>
<td>Biphase_S</td>
<td><img src="image" alt="Waveform" /></td>
<td></td>
</tr>
</tbody>
</table>
DATA MODULATION

Although all the data is transferred to the host by amplitude-modulating the carrier (backscatter modulation), the actual modulation of 1's and 0's is accomplished with three additional modulation methods:

1. **Direct.** In direct modulation, the Amplitude Modulation of the backscatter approach is the only modulation used. A high in the envelope is a ‘1’ and a low is a ‘0’. Direct modulation can provide a high data rate but low noise immunity.

2. **FSK (Frequency Shift Keying).** This form of modulation uses two different frequencies for data transfer; the most common FSK mode is Fc/8/10. In other words, a ‘0’ is transmitted as an amplitude-modulated clock cycle with period corresponding to the carrier frequency divided by 8, and a ‘1’ is transmitted as an amplitude-modulated clock cycle period corresponding to the carrier frequency divided by 10. The amplitude modulation of the carrier thus switches from Fc/8 to Fc/10 corresponding to 0's and 1's in the bitstream, and the reader has only to count cycles between the peak-detected clock edges to decode the data. FSK allows for a simple reader design, provides very strong noise immunity, but suffers from a lower data rate than some other forms of data modulation. In Figure 3, FSK data modulation is used with NRZ encoding.

3. **PSK (Phase Shift Keying).** This method of data modulation is similar to FSK, except only one frequency is used, and the shift between 1’s and 0’s is accomplished by shifting the phase of the backscatter clock by 180 degrees. Two common types of PSK are:
   - Change phase at any ‘0’, or
   - Change phase at any data change (0 to 1 or 1 to 0).

PSK provides fairly good noise immunity, a moderately simple reader design, and a faster data rate than FSK. Typical applications utilize a backscatter clock of Fc/2, as shown in Figure 4.
ANTICOLLISION

In many existing applications, a single-read RFID tag is sufficient and even necessary: animal tagging and access control are examples. However, in a growing number of new applications, the simultaneous reading of several tags in the same RF field is absolutely critical: library books, airline baggage, garment, and retail applications are a few.

In order to read multiple tags simultaneously, the tag and reader must be designed to detect the condition that more than one tag is active. Otherwise, the tags will all backscatter the carrier at the same time, and the amplitude-modulated waveforms shown in Figures 3 and 4 would be garbled. This is referred to as a collision. No data would be transferred to the reader. The tag/reader interface is similar to a serial bus, even though the “bus” travels through the air. In a wired serial bus application, arbitration is necessary to prevent bus contention. The RFID interface also requires arbitration so that only one tag transmits data over the “bus” at one time.

A number of different methods are in use and in development today for preventing collisions; most are patented or patent pending, but all are related to making sure that only one tag “talks” (backscatters) at any one time. See the MCRF355/360 Data Sheet (page 7) and the 13.56 MHz Reader Reference Design (page 47) chapters for more information regarding the MCRF355/360 anticollision protocol.
Note the following details of the code protection feature on PICmicro® MCUs.

- The PICmicro family meets the specifications contained in the Microchip Data Sheet.
- Microchip believes that its family of PICmicro microcontrollers is one of the most secure products of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the PICmicro microcontroller in a manner outside the operating specifications contained in the data sheet. The person doing so may be engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable".
- Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our product.

If you have any further questions about this matter, please contact the local sales office nearest to you.

Information contained in this publication regarding device applications and the like is intended through suggestion only and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. No representation or warranty is given and no liability is assumed by Microchip Technology Incorporated with respect to the accuracy or use of such information, or infringement of patents or other intellectual property rights arising from such use or otherwise. Use of Microchip's products as critical components in life support systems is not authorized except with express written approval by Microchip. No licenses are conveyed, implicitly or otherwise, under any intellectual property rights.

Microchip received QS-9000 quality system certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona in July 1999. The Company's quality system processes and procedures are QS-9000 compliant for its PICmicro® 8-bit MCUs, KEELOQ® code hopping devices, Serial EEPROMs and microperipheral products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001 certified.

Trademarks

The Microchip name and logo, the Microchip logo, FilterLab, KEELOQ, microID, MPLAB, PIC, PICmicro, PICMASTER, PICSTART, PRO MATE, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.
dsPIC, ECONOMONITOR, FanSense, FlexROM, fuzzyLAB, In-Circuit Serial Programming, ICSP, ICEPIC, microPort, Migratable Memory, MPASM, MPLIB, MPLINK, MPSIM, MXDEV, PICC, PICDEM, PICDEM.net, rFIC, Select Mode and Total Endurance are trademarks of Microchip Technology Incorporated in the U.S.A.

Serialized Quick Turn Programming (SQTP) is a service mark of Microchip Technology Incorporated in the U.S.A.

All other trademarks mentioned herein are property of their respective companies.

© 2002, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

Printed on recycled paper.