Final Project
Introduction to RFID
(Radio Frequency IDentification)

Andreas G. Andreou
Radio Frequency IDentification

- Tag wirelessly sends bits of data when it is triggered by a reader
- Power source not required for passive tags... a defining benefit
- Superior capabilities to barcode:
  - Non Line of Sight
  - Hi-speed, multiple reads
  - Can read and write to tags
  - Unit specific ID

<table>
<thead>
<tr>
<th>Four main frequencies:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frequency</strong></td>
</tr>
<tr>
<td>LF</td>
</tr>
<tr>
<td>HF</td>
</tr>
<tr>
<td>UHF</td>
</tr>
<tr>
<td>µwave</td>
</tr>
</tbody>
</table>
Lecture Objectives:

- Explain technical principles behind RFID
- Provide overview of RFID technology
- Discuss architecture for RFID chips
Outline

• RFID history
• Technical principles
• Tag overview
• Reader overview
• Adoption challenges
• The UHF market
• The future??
RFID History

• First Bar code patents – 1930s
• First use of RFID device – 2\textsuperscript{nd} world war – Brittan used RFID-like technology for Identify- Friend or Foe
• Harry Stockman October 1948 Paper – Communication by means of reflected power (The proceedings of the Institute of Radio Engineers)
• First RFID Patent - 1973
• Auto-ID center founded at MIT – 1999
  – Standardization effort taken over by EPC Global (Electronic Product Code)
• Current thrust primarily driven by Wal-Mart and DoD
  – Automate Distribution:
    • Reduce cost (man power, shipping mistakes)
    • Increase sales (keep shelves full)
    • DoD Total Asset Visibility Initiative

Source of data: EDN – October 2004 - “Reading Between the Lines” Brian Dipert
Basic Tag Operational Principles

- **Near field (LF, HF):** inductive coupling of tag to magnetic field circulating around antenna (like a transformer)
  - Varying magnetic flux induces current in tag. Modulate tag load to communicate with reader
  - Field energy decreases proportionally to $1/R^3$ (to first order)
- **Far field (UHF, microwave):** backscatter.
  - Modulate backscatter by changing antenna impedance
  - Field energy decreases proportionally to $1/R$
- **Boundary between near and far field:** $R = \text{wavelength}/2\pi$, so, once have reached far field, lower frequencies will have lost significantly more energy than high frequencies
- **Absorption by non-conductive materials** significant problem for microwave frequencies

Source of data: "Introduction to RFID" CAENRFID an IIT Corporation
Basic Principle
Traditional RFID Market Segments

Auto Immobilizers

- Isolated systems
- Simple reads
- Slow growth

Access Control

Automated Vehicle Id

Animal Tracking
The New Mkt Segment
Consumer Pkg Goods Supply Chain

Wal-Mart
- June ’03 announcement
- Pallet/Case tagging
  - Top 100 suppliers Jan ’05
  - Other 30K by end of ’06
- 4 Billion tags/year
- 300k direct readers
- 18 Million indirect readers

• End to end systems
• Complex reads
• Emerging market
Usage Models

- Dock Door
- Conveyor Belt
- Forklift
- Printers
- Handheld
- Smart Shelves
- Point of Sale
Tags
Types of Tags

- **Passive**
  - Operational power scavenged from reader radiated power

- **Semi-passive**
  - Operational power provided by battery

- **Active**
  - Operational power provided by battery - transmitter built into tag
Generic Tag Architecture
(Highly Simplified)
What is on a chip

Architecture of a $\mu$RFID with integrated antenna in 3D SOI-CMOS

Edward Choi* and Andreas Andreou*
*Department of Electrical and Computer Engineering
The Johns Hopkins University, Baltimore, MD
Email: echoi, andreou@jhu.edu
RFID Antennas:

- Gate antennas (orthogonal use)
- Patch antennas
- Circular polarized
- Omni directional antennas
- Stick antennas (directional)
- Di-pole or multi-pole antennas
- Linear polarized
- Adaptive, beam-forming or phased-array element antennas
Electronic Product Code

EPC Data Standard - 96 bit

With 96 bit code, 268 million companies can each categorize 16 million different products where each product category contains up to 687 billion individual units.

Header - Tag version number
EPC Manager - Manufacturer ID
Object class - Manufacturer’s product ID
Serial Number - Unit ID

Note: 64 bit versions also defined, 256 bit version under definition
<table>
<thead>
<tr>
<th></th>
<th>LF</th>
<th>HF</th>
<th>UHF</th>
<th>Microwave</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Freq. Range</strong></td>
<td>125 - 134KHz</td>
<td>13.56 MHz</td>
<td>866 - 915MHz</td>
<td>2.45 - 5.8 GHz</td>
</tr>
<tr>
<td><strong>Read Range</strong></td>
<td>10 cm</td>
<td>1M</td>
<td>2-7 M</td>
<td>1M</td>
</tr>
<tr>
<td><strong>Market share</strong></td>
<td>74%</td>
<td>17%</td>
<td>6%</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Coupling</strong></td>
<td>Magnetic</td>
<td>Magnetic</td>
<td>Electro magnetic</td>
<td>Electro magnetic</td>
</tr>
<tr>
<td><strong>Existing standards</strong></td>
<td>11784/85, 14223</td>
<td>18000-3.1,</td>
<td>EPC C0, C1, C1G2,</td>
<td>18000-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15693, 14443 A, B, and C</td>
<td>18000-6</td>
<td></td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Smart Card, Ticketing, animal tagging, Access, Laundry</td>
<td>Small item management, supply chain, Anti-theft, library, transportation</td>
<td>Transportation vehicle ID, Access/Security, large item management, supply chain</td>
<td>Transportation vehicle ID (road toll), Access/Security, large item management, supply chain</td>
</tr>
</tbody>
</table>
## Competing UHF Protocols (EPC only)

<table>
<thead>
<tr>
<th></th>
<th>Read Rate</th>
<th>Read or Read/Write</th>
<th>Tag Cost</th>
<th>Privacy</th>
<th>Security</th>
<th>Global Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class 0</strong></td>
<td>NA: 800 reads/sec</td>
<td>Read Only</td>
<td>$$</td>
<td>24 bit password</td>
<td>Reader broadcasts OID or Anonymous modes with reduced throughput</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>EU: 200 reads/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Class 0+</strong></td>
<td>NA:800 reads/sec</td>
<td>Read &amp; Write</td>
<td>$$</td>
<td>See above</td>
<td>See above</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>EU:200 reads/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Class 1</strong></td>
<td>NA:200 reads/sec</td>
<td>Read &amp; Write</td>
<td>$</td>
<td>8 bit password</td>
<td>Reader broadcasts partial OID</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>EU: 50 reads/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em><em>Class 1 Gen 2</em> (UHF Gen2)</em>*</td>
<td>NA:1700 reads/sec</td>
<td>Read &amp; Write</td>
<td>? 32 bit password and concealed mode</td>
<td>Authentication and Encryption</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EU: 600 reads/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Class 1 Gen 2 is still in development, expected to close in Q4, 2004
Class 0 Protocol

<table>
<thead>
<tr>
<th>Backscatter</th>
<th>North America</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 0 Tag Backscatter Frequency</td>
<td>3.3 Mhz for data &quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>2.2 Mhz for data &quot;0&quot;</td>
</tr>
<tr>
<td>Modulation Format</td>
<td>FSK</td>
</tr>
</tbody>
</table>

Typical data stored in tag:

- 96 bit EPC code
- 24 bit kill code
- 16 bit Cyclic Redundancy Check (CRC)

Reader/tag communication modes:

1. Start up signals (power up tags and sync. with them)
2. Tree Traversal (read individual tags)
3. Communication (send commands to tags)

Data rates: fast and slow defined: fast (12.5 micro sec bit period) and slow (62.5 micro second bit period) --- either 20% or 100% modulation depths
Class 0 Signaling

EPC: Reader-tag Communication

- Reader to tag communication (AM)
  - Output RF power is modulated between full and fractional power
  - 50% duty cycle is binary ‘1’
  - 88% duty cycle is binary ‘0’
    - Picture at left shows ‘01’
      - Tag to reader communication

- Tag responds by FM
  - 2 cycles of modulation in one data bin is a binary ‘1’
  - 1 cycle of modulation is a binary ‘0’
    - Picture at left shows ‘1011’
Basic Architecture

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>130 kHz</td>
</tr>
<tr>
<td>Modulation type</td>
<td>100% ASK</td>
</tr>
<tr>
<td>Modulation frequency/modulation signal</td>
<td>12.5 Hz or 25 Hz, rectangle 50%</td>
</tr>
</tbody>
</table>
Default Class 0 Reader Communication Sequence

Tag power up, reset, and calibration process

Reader power up

- Power Up
- Master Reset
- Oscillator Calibration
- Data Calibration
- Global cmds

Reader Transmit Once Only

Repeated after each frequency hop

- Reset: 800 micro sec uninterrupted continuous wave
- Oscillator calibration: 8 116 micro sec pulses
- Data calibration: 3 pulses (data “0”, data “1”, data “null”)

Tag Singulation Process

- BT

Repetitive Binary Traversals

Single Binary Transversal

- msb Identification Number lsb
- Header Manager, Product and Serial Numbers

ID length = 64, 96 bits
CRC = 16 bits
Total Tag ID Length = 80, 112 bits

Once tag has been singulated, reader can send commands to it or begin next BT cycle
Tag Singulation Process
read individual tag from group of all tags in range of reader

Basic process:

1. All tags within range of reader backscatter their MSB to the reader.

2. Reader responds with either a 1 or a 0.

3. If tag bit equals reader bit, tag backscatters the next bit in its code. If instead, tag bit does not equal reader bit, tag goes mute for remainder of singulation.

4. Process continues until reader has completely read a single tag.

5. Reader conducts consecutive singulations until all tags in its range are read.

6. Reader can interrupt the singulation process to send commands to a single tag, a subset of all tags in range, or globally to all tags in range.
Readers
Close coupled magnetic reader
Close coupled capacitive reader
## UHF Reader Standards

<table>
<thead>
<tr>
<th>GEO / Country</th>
<th>Frequency Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>900 – 930 MHz</td>
</tr>
<tr>
<td>EMEA</td>
<td>866 – 868 MHz</td>
</tr>
<tr>
<td>Korea</td>
<td>908.5 – 914 MHz</td>
</tr>
<tr>
<td>Australia</td>
<td>918 – 926 MHz</td>
</tr>
<tr>
<td>China (PRC)</td>
<td>TBD</td>
</tr>
<tr>
<td>Japan</td>
<td>TBD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transmitter</th>
<th>North America</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Freq. Band</td>
<td>902 – 928 Mhz</td>
</tr>
<tr>
<td>Output Power</td>
<td>4 watts EIRP</td>
</tr>
<tr>
<td>TX Channel step</td>
<td>500Khz</td>
</tr>
<tr>
<td>Hop frequency</td>
<td>2.5 to 20 times per second</td>
</tr>
<tr>
<td>TX Channels</td>
<td>902.75, 903.25, ..., 927.25MHz</td>
</tr>
<tr>
<td>Modulation</td>
<td>Typically ASK — 20% to 100% modulation depth</td>
</tr>
</tbody>
</table>

Note: EIRP = 1.64X ERP (Effective Radiated Power)
Reader Implementation Challenges

• Reader must deliver enough power from RF field to power the tag

• Reader must discriminate backscatter modulation in presence of carrier at same frequency

• 70db magnitude difference between transmitted and received signals

• Interference between readers

• Hugh volume of tag data – readers need to filter data before releasing to enterprise network
RFIDs Today!

- **Cost:**
  - Tags - currently 50 cents – need to be 5 cents or less
  - Readers – currently thousands of dollars – need to be hundreds of dollars
  - Implementation – distribution centers relatively low tech – need networking, power, etc.
    - Cost benefit - must be significant enough to justify RFID cost:
      - Retailers operate with small margins ( < 5%). If RFID can increase operational efficiency by 1% = major competitive advantage

- **Read accuracy:**
  - accuracy not established – needs to approach 100%:
    - Metal containers, liquids, Etc. impact tag readability
    - Taq/reader orientation: polarization effects
    - Reader configuration: cooperative networks of readers
    - Interference from other readers and other radiators

- **Design Robustness:**
  - Needs to be robust enough to survive/function in warehouse environments

- **Security:**
  - Read security, Data security, etc.

- **Privacy:**
  - See next slide
The Future

• What fundamental changes does RFID herald in?

• What are the probable consequences of these changes?
Protocol Details
Class 0 Tag Start-up Signals:
Reset and Oscillator Calibration

- **Reset**
  - Total time: 800 microseconds

- **Oscillator Calibration Signals**
  - 8 pulses (t) each of 116 microseconds shown in blue.
  - Pulse separations (s): 6μsec RF off, 6μsec RF on, min., shown in green
Class 0 Tag Start-up Signals:
Data Calibration

Data Calibration and Data Transmission Signals

Timing for Data Event Points

Data '0', '1', and 'null': Data Calibration Signals
to be interpreted

(mid 0/1 bit) (mid 0/null bit) (tag Tx off)
Reader Bit Definitions

**Reader bit '0' (fast bit rate)**
Total bit exchange time - 12.5 µs, typ.

- 3µs
- 1.2µs reader Tx delay
- 1/2 bit cycle for reference
- response end from tags

**Reader bit '1' (fast bit rate)**
Total bit exchange time 12.5 µs, typ.

- 6µs
- 1.2µs reader Tx delay
- 1/2 bit cycle for reference
- response end from tags

**Reader 'null' bit (fast bit rate)**
Total bit exchange time 12.5 µs, fast mode

- 9.5µs
- 1/2 bit cycle for reference
- (No tag response)
Tag Backscatter

Tag Backscatter on Reader Data Symbol
Total bit exchange time

Clock start
1-2μs reader
Tx delay
response start from tags
Tag response
response end from tags
Possible Reader/Tag Communication Pairs

Tag (green) bit '0' on Reader (blue) bit '0' (fast mode)
Total bit exchange time 12.5 μs, typ.

Clock start
1-2 μs reader Tx delay
4 μs - 5 μs response start from tags
6 μs
11.5 μs response end from tags

Tag response (6.5 ± 7.5 μs) of 2.25 MHz
(16-18 cycles)

Tag (green) bit '1' on Reader (blue) bit '0' (fast mode)
Total bit exchange time 12.5 μs, typ.

Clock start
1-2 μs reader Tx delay
4 μs - 5 μs response start from tags
6 μs
11.5 μs response end from tags

Tag response (6.5 ± 7.5 μs) of 3.25 MHz
(24-28 cycles)

Tag (green) bit '0' on Reader (blue) bit '1' (fast mode)
Total bit exchange time 12.5 μs, typ.

Clock start
1-2 μs reader Tx delay
7 μs - 8 μs response start from tags
6 μs
11.5 μs response end from tags

Tag response (3.5 ± 4.5 μs) of 2.25 MHz
(8-11 cycles)

Tag (green) bit '1' on Reader (blue) bit '1' (fast mode)
Total bit exchange time 12.5 μs, typ.

Clock start
1-2 μs reader Tx delay
7 μs - 8 μs response start from tags
6 μs
11.5 μs response end from tags

Tag response (3.5 ± 4.5 μs) of 3.25 MHz
(13-18 cycles)

Tag (green) bit '0' on Reader (blue) bit '0' (slow mode)
Total bit exchange time 25 μs (slow mode).

Clock start
3 μs
6 μs
24 μs response end from tags

Tag response (20 μs) of 2.25 MHz
(50 cycles)