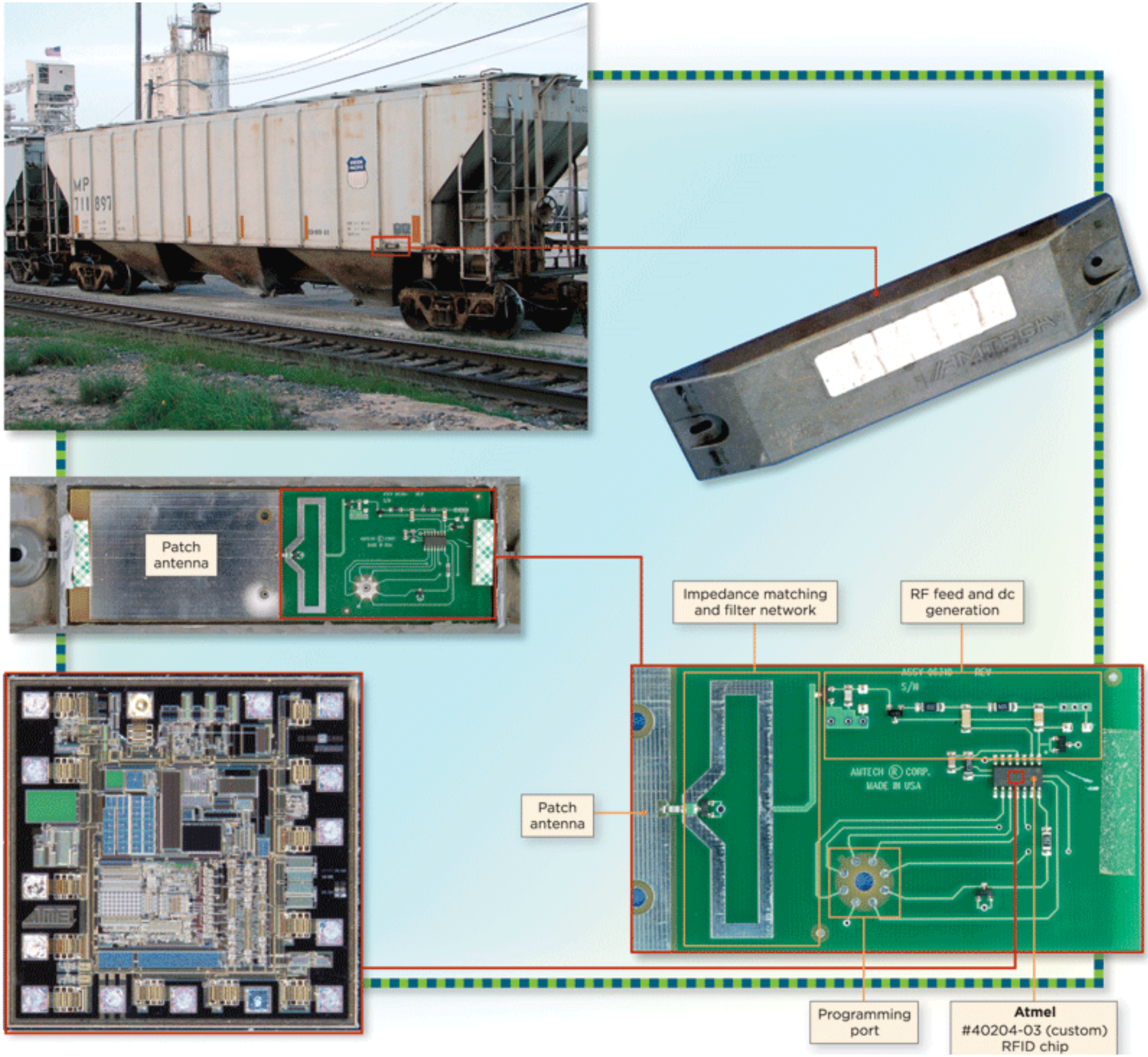
RFID

iCLASS®

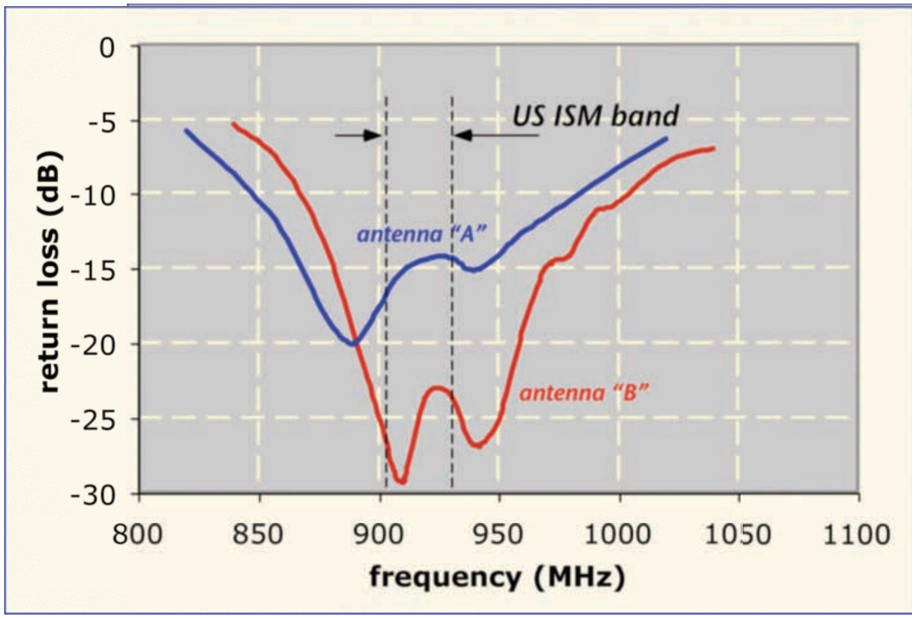
Optimized to make physical access control more powerful, iCLASS® 13.56 MHz read/write contactless smart card technology provides versatile interoperability and supports multiple applications such as biometric authentication, cashless payment and PC log-on security.

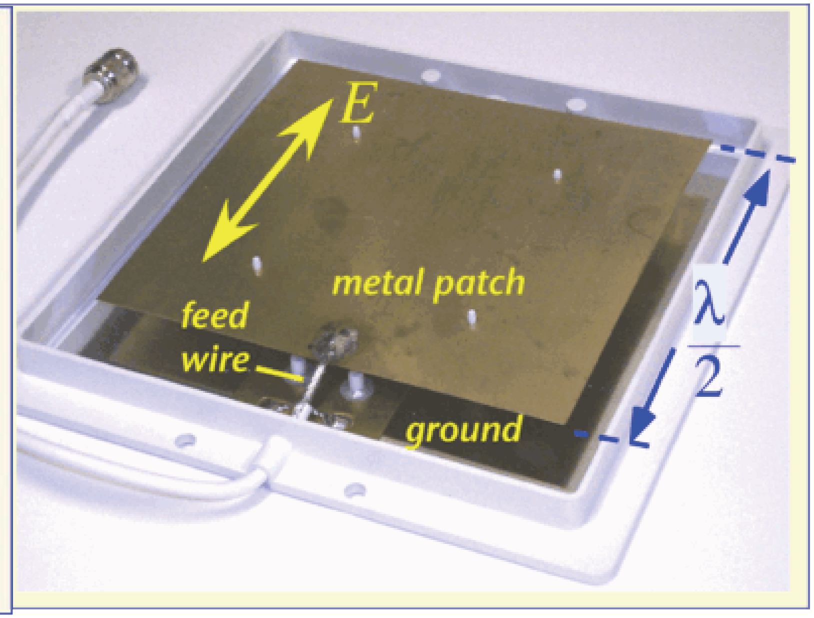
HID® The Trusted Source for Secure Identity Solutions

http://www.hidglobal.com


Patch antenna
Impedance matching and filter network
RF feed and dc generation
Patch antenna
Programming port
Atmel #40204-03 (custom) RFID chip

Patch Antenna





US Industrial, Scientific, and Medical (ISM) band
from 902-928 MHz

$$\frac{\delta f}{f_{res}} = \frac{Z_0}{2R_{rad}}\frac{d}{W} = 1.2\left(\frac{d}{W}\right)$$

Atmel

Products | Applications | Technologies | Video | About Atmel | Buy

Find It
Documents
Tools
Products
By Device
- Microcontrollers (444)
- Touch Solutions (36)
- Memory (118)
- Automotive (177)
- Wireless (54)
- More Products (180)

By Application
- Automotive
- Building Automation
- Home Appliances
- Home Entertainment
- Industrial Automation
- Lighting
- More

- List View
- Parametric Table

Find

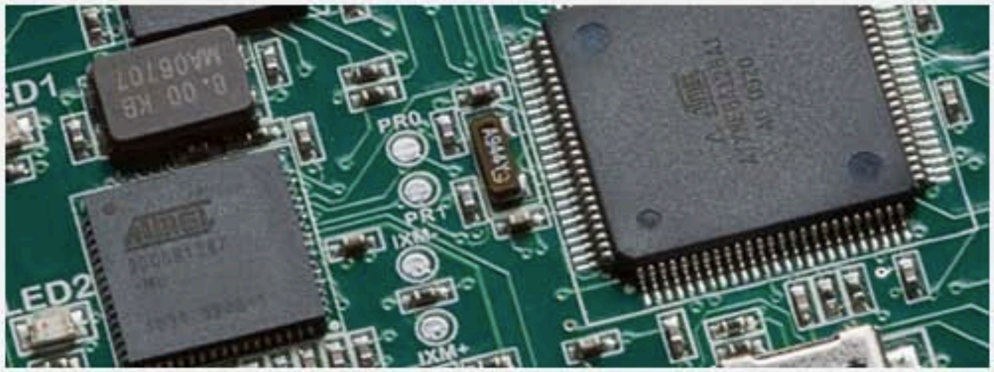
Microcontrollers
Touch Solutions
Memory
Automotive
Wireless / RF
MCU Wireless
RF Identification
100-150 kHz AVR RFID Reader ICs
100-150 kHz OTP
100-150 kHz Read/Write
100-150 kHz Reader ICs
125 kHz Transponder
Active RFID
Smart RF
Wi-Fi
More Products

Home > Products > Wireless / RF > RF Identification

SHARE Print

RF Identification

Overview | Parameters | Documents | Tools



Secure, Sensitive, Low Power Identification Devices

RFID involves contactless reading and writing of data into an RFID tag's nonvolatile memory through an RF signal. Low frequency RFID devices typically consist of a transponder (tag) and reader.

To help you reach the extensive vertical markets that rely on RFID, we offer a complete line of contactless products. Our transponders and readers operate within the 100 to 150 kHz and 13.56 MHz bandwidth ranges. Our RFID chips are suitable for the smallest devices and require few external components, lowering your system costs. Rugged architecture with excellent noise suppression increases reliability and usability in both indoor and outdoor environments.

You can choose from a broad range of read or read/write devices, available as identification ICs on die on wafer, die in tray, die on tape, or micromodule, to complete transponders in plastic packaging with reader, tag and development library.

Key Features

- **Standards based** — You can rely on the fact that Atmel complies to industry-specific standards, such as ISO 11784/85 (FDX-B and FDX-A) for agriculture and ISO 14443 for public transportation applications.
- **Flexible modulation coding options** — The chips can be easily configured to suit a broad array of modulation schemes: FSK, PSK ,ASK, Manchester, Bi-phase, NRZ direct coding, and more.

Get Started

We'll tell you all you need to know to start evaluating and working with this product.

» **Start Now**
» **Contact Sales**
» **Request Samples**
» **Sign-Up for News**

Related Items

» Overview
» Third Party Support
» RF Identification FAQs
» Technical Support
» What's Changed
» Mature Devices

LF RFID Application Kit ATA2270-EK1 tool card
» Learn More

There's a reason why Tadiran batteries were chosen for E-ZPass, the world's best known RFID application

When millions of motorists across the United States flash their E-ZPass at toll booths, they are totally unaware that this pioneering RFID technology is powered by Tadiran lithium batteries. Manufacturers of these electronic toll tags require a battery capable of delivering years of safe, reliable and trouble-free performance under the toughest of environmental conditions, as automotive windshields are subjected to extreme heat, vibration and rapid temperature changes. So they naturally turn to Tadiran.

Tadiran lithium thionyl chloride batteries were also selected by Awarepoint for the medical industry's first 24/7 RFID asset tracking system. Awarepoint required a battery capable of withstanding extreme autoclave and chemical sterilization temperatures, so they chose Tadiran lithium thionyl chloride batteries that deliver unrivaled performance under the most extreme environmental conditions.

Tadiran batteries feature the highest energy density (1,420 Wh/l), high capacity, and are uniquely able to withstand extreme temperatures (-55°C to +125°C), and offer 20+ year service life due to extremely low self-discharge (less than 1% per year). These batteries are also designed with unique safety features that protect the cell against extreme temperature, pressure, puncture, shock and vibration.

If your RFID application calls for an extended-life battery, don't settle for anything less than Tadiran, as no one can match our experience and our proprietary manufacturing methods.

Would you like to complete our [application questionnaire?]

Related Articles

Batteries in medical RFID: Withstanding the heat of autoclaves is a must
PDF Version

May the power be with you: Improving the performance of RFID solutions
(as appeared in Global ID).
PDF Version

Contactless ID

iCLASS®

Optimized to make physical access control more powerful, iCLASS® 13.56 MHz read/write contactless smart card technology provides versatile interoperability and supports multiple applications such as biometric authentication, cashless payment and PC log-on security.

http://www.hidglobal.com

Features

Read/write Functionality for Multi-functional Memory Applications

iCLASS® was specifically designed to make access control more powerful, more versatile, and more secure. All radio frequency data transmission between the card and reader is encrypted using a secure algorithm. By using industry standard encryption techniques, iCLASS reduces the risk of compromised data or duplicated cards. For even higher security, the card data may also be protected with DES or triple DES encryption. Multiple securely separated application areas are each protected by 64-bit diversified read/write keys which allow complex applications and provide for future expansion.

Security mechanisms such as mutual authentication and encryption are efficiently combined with fast processing and data communication, resulting in transaction times of less than 100 milliseconds for a typical secure e-purse transaction.

Proven, Reliable Technology

Offers extremely consistent read range. Unaffected by body shielding or variable environmental conditions.

Thin

Can be carried with credit cards in a wallet or purse. Use with a strap and clip as a photo ID badge.

*** Photo ID Compatible**

Print directly to the card with a direct image or thermal transfer printer. Slot punch vertically for easy use.

Long Life

Passive, no-battery design allows for an estimated minimum 100,000 reads.

Durability

Strong, flexible, and resistant to cracking and breaking.

Options:

- Magnetic stripe
- External card numbering (inkjet or laser engraving)
- Vertical slot punch
- Custom artwork (text or graphics)
  (Please see "How To Order Guide" for a description of the options and associated part numbers.)

Warranty

Lifetime warranty. See complete warranty policy for details.

Base Part Numbers

- 2000 for 2k bit (256 Byte) card
- 2001 for 16k bit (2k Byte) card with 2 application areas
- 2002 for 16k bit (2k Byte) card with 16 application areas
- 2003 for 32k bit (4k Byte) 16k/2+16k/1.
- 2004 for 32k bit (4k Byte) 16k/16 + 16k/1.

Description

13.56 MHz contactless smart card.

HID iCLASS Contactless Smart Card presentation - YouTube

Specifications

Typical Maximum Read Range*

R10 2.0-3.0" (5.0-7.6cm)
R30/RW300 2.0-3.5" (5.0-8.9cm)
R40/RW400 2.5-4.5" (6.3-11.4cm)
RK40/RWK400 3.0-4.0" (7.6-10.1 cm)
*Dependent upon installation conditions.

Dimensions

2.127" x 3.375" x 0.033" max. (5.40 x 8.57 x 0.084 cm)

Weight

0.20oz (5.7 g)

Card Construction

Thin, flexible polyvinyl chloride (PVC) laminate.

Operating Temperature

-40° to 158° F (-40° to 70° C)

Operating Humidity

5-95% non-condensing

Operating Frequency

13.56 MHz

RF Interface

As suggested by ISO/IEC:
15693 read/write
14443B mode - 106 kbps

Transaction Time

<100 ms typical

Baud Rate

14443 B2 mode - 212 kbps
15693 mode - 26 kbps

Memory Type

EEPROM, read/write

Multi-application Memory

2k bit (256 Byte) card – 2 application areas
16k bit (2k Byte) card – 2 or 16 application areas
32k bit (4k Byte) card – 16k bits in 2 or 16 application areas plus 16k bits user configurable.

Write Endurance

About 70¢/Card

Fr | Ru Members St

Standards About us Standards Development News

Search ISO

Standards catalogue Publications and e-products

ISO Store > Standards catalogue > By ICS > JTC 1 Information technology > SC 17

RSS

ISO/IEC 15693-1:2010

Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics

Media and price

Format	Price	Language	
PDF	CHF 50,00	English	Add to basket
Paper	CHF 50,00	English	Add to basket

Abstract

ISO/IEC 15693-1:2010 defines the physical characteristics of vicinity cards (VICCs). It is used in conjunction with other parts of ISO/IEC 15693.

Contact custom

Send your enquiry by

or call us on +41 22 7

09:00 – 12:30, 14:00 -

Related standar

Standards in the same

Standards from the sa

www.waazaa.org » 15693

ISO/IEC 15693 : Vicinity cards

ISO 15693 is an international standard for « Vicinity Cards », i.e. contactless cards operating at the 13.56 MHz frequency, with a maximum operating distance of 1 to 1.5 metres.

The standard

These documents are Final Comittee Drafts. They are not the official documents (which must be purchased from ISO or from your national standardization agency), but are very close to them.

- 15693-1 : Physical characteristics
- 15693-2 : Radio frequency power and signal interface
- 15693-3 : Anticollision and transmission protocol
- 10373-7 : Test methods

Identification cards - Contactless integrated circuit(s) cards - Vicinity cards

Part 2: Radio frequency power and signal interface

1 Scope

This part of ISO/IEC 15693 specifies the nature and characteristics of the fields to be provided for power and bi-directional communications between vicinity coupling devices (VCDs) and vicinity cards (VICCs).

This part of ISO/IEC 15693 shall be used in conjunction with other parts of ISO/IEC 15693.

This part of ISO/IEC 15693 does not specify the means of generating coupling fields, nor the means of compliance with electromagnetic radiation and human exposure regulations which can vary according to country.

6 Power transfer

Power transfer to the VICC is accomplished by radio frequency via coupling antennas in the VCD and in the VICC. The RF operating field that supplies power to the VICC from the VCD is modulated for communication from the VCD to the VICC, as described in clause 7.

6.1 Frequency

The frequency (f_c) of the RF operating field is 13,56 MHz ±7 kHz.

6.2 Operating field

A VICC shall operate as intended continuously between H_{min} and H_{max}.

The minimum operating field is H_{min} and has a value of 150 mA/m rms.

The maximum operating field is H_{max} and has a value of 5 A/m rms.

A VCD shall generate a field of at least H_{min} and not exceeding H_{max} at manufacturer specified positions (operating volume).

In addition, the VCD shall be capable of powering any single reference VICC (defined in the test methods) at manufacturer's specified positions (within the operating volume).

The VCD shall not generate a field higher than the value specified in part 1 of ISO/IEC 15693 (alternating magnetic field) in any possible VICC position.

7 Communications signal interface VCD to VICC

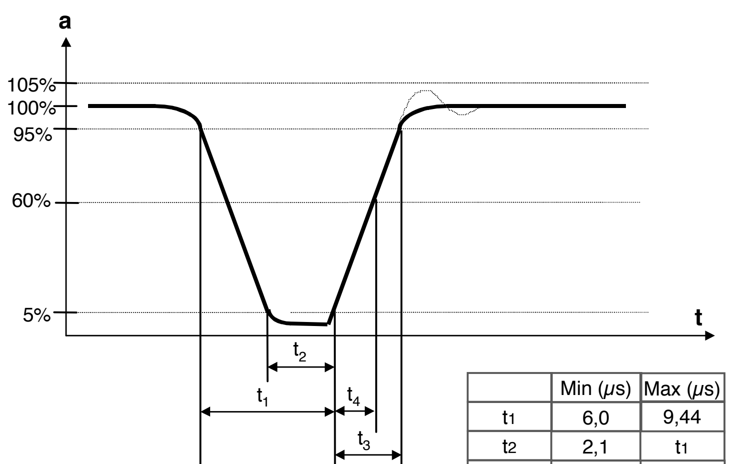
For some parameters several modes have been defined in order to meet different international radio regulations and different application requirements.

From the modes specified any data coding can be combined with any modulation.

7.1 Modulation

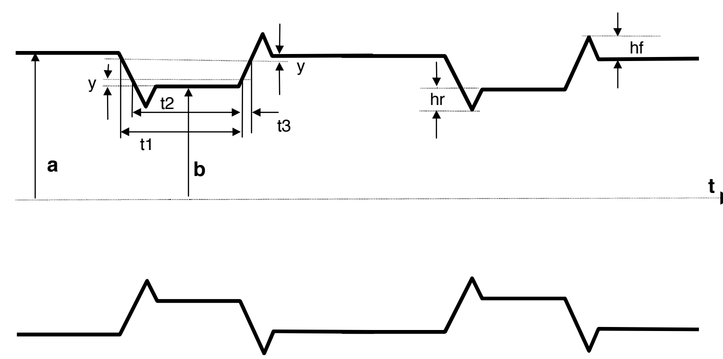
Communications between the VCD and the VICC takes place using the modulation principle of ASK. Two modulation indexes are used, 10% and 100%. The VICC shall decode both. The VCD determines which index is used.

Depending of the choice made by the VCD, a "pause" will be created as described in Figures 1 and 2.



	Min (µs)	Max (µs)
t1	6,0	9,44
t2	2,1	t1
t3	0	4,5
t4	0	0,8

Figure 1: 100% Modulation Waveform



	Min	Max
t1	6,0 µs	9,44 µs
t2	3,0 µs	t1
t3	0	4,5 µs
Modulation Index	0.1	0.3

y	0,05 (a-b)
hf, hr	0,1 (a-b) max

The clock recovery must be operational after t_4 max

Figure 2: 10% Modulation Waveform

7.2 Data rate and data coding

Data coding shall be implemented using pulse position modulation.

Two data coding modes shall be supported by the VICC. The selection shall be made by the VCD and indicated to the VICC within the Start of frame (SOF). See 7.3.

8 Communications signal interface VICC to VCD

For some parameters several modes have been defined in order to allow for use in different noise environments and application requirements.

8.1 Load modulation

The VICC shall be capable of communication to the VCD via an inductive coupling area whereby the carrier is loaded to generate a subcarrier with frequency f_s. The subcarrier shall be generated by switching a load in the VICC.

The load modulation amplitude shall be at least 10 mV when measured as described in the test methods.

Test methods for VICC load modulation are defined in International Standard ISO/IEC 10373.

8.4.1 Bit coding when using one subcarrier

A logic 0 starts with 8 pulses of 423,75 kHz (f_c/32) followed by an unmodulated time of 18,88 μs (256/f_c). As shown in Figure 10.

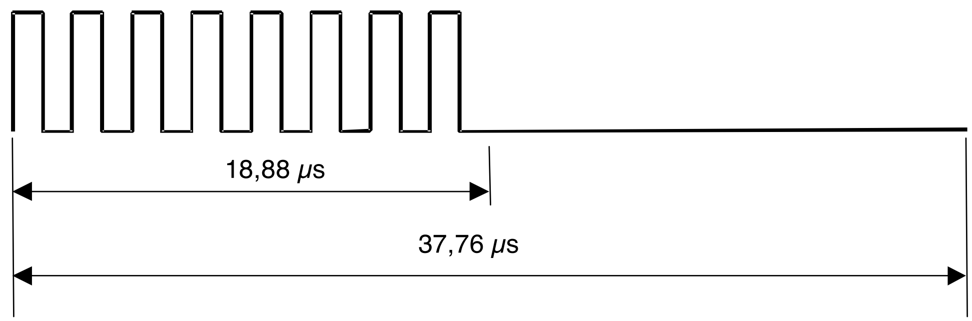


Figure 10: Logic 0

A logic 1 starts with an unmodulated time of 18,88 μs (256/f_c) followed by 8 pulses of 423,75 kHz (f_c/32). As shown in Figure 11.

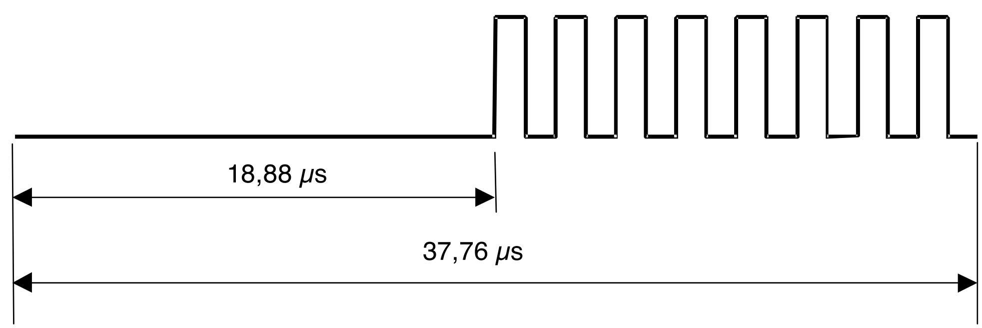


Figure 11: Logic 1

A greatly simplified diagram of the electrical constituents of a passive tag is depicted in Figure 5.1. The radio signal at around 900 MHz from the reader is converted by the antenna into an alternating current, from which the tag must extract both power and information. The tag must then interpret the resulting data, possibly requiring writing data to nonvolatile memory, and modulate the load presented to the antenna in order to change the backscattered signal returning to the reader.

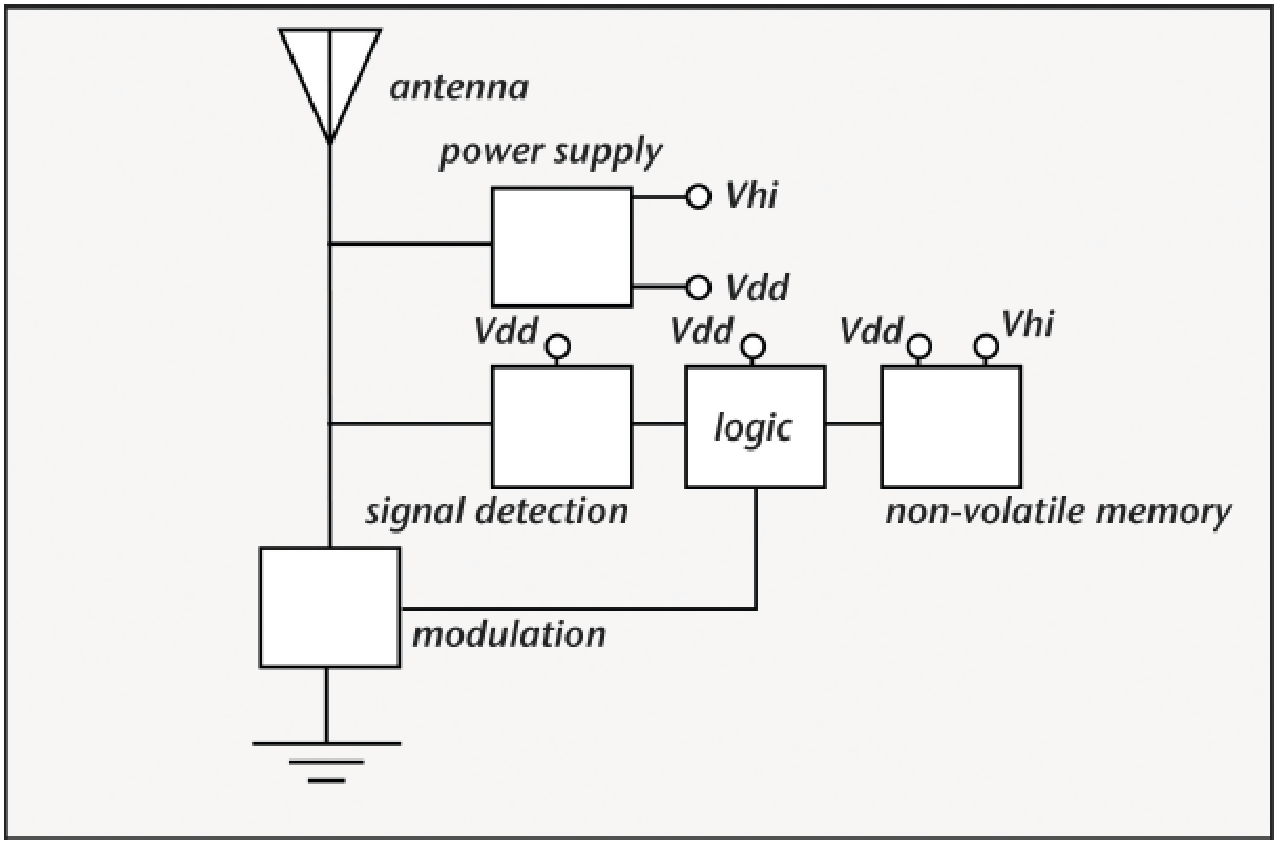


Figure 5.1: Elements of a Passive UHF Tag.

In what follows, we shall examine a few of the special challenges of designing and manufacturing a passive UHF tag:

- How is power to be extracted from the high-frequency radio signal?
- How can we simultaneously acquire whatever data the reader has sent?
- How do we send back information to the reader?
- How is the resulting chip designed and fabricated?
- How is a completed tag assembled from the chip and other parts?

http://rfid.net/basics/passive/137-uhf-rfid-tags

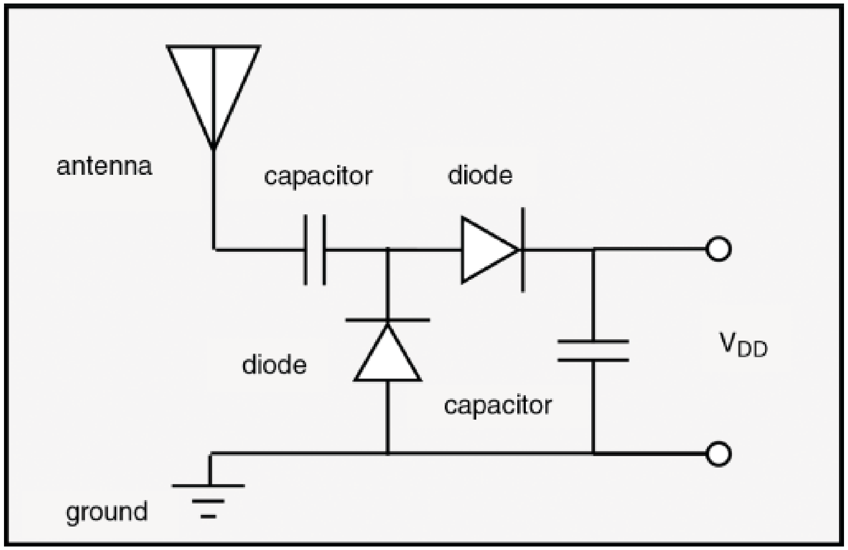


Figure 5.6: Voltage Doubler Schematic.

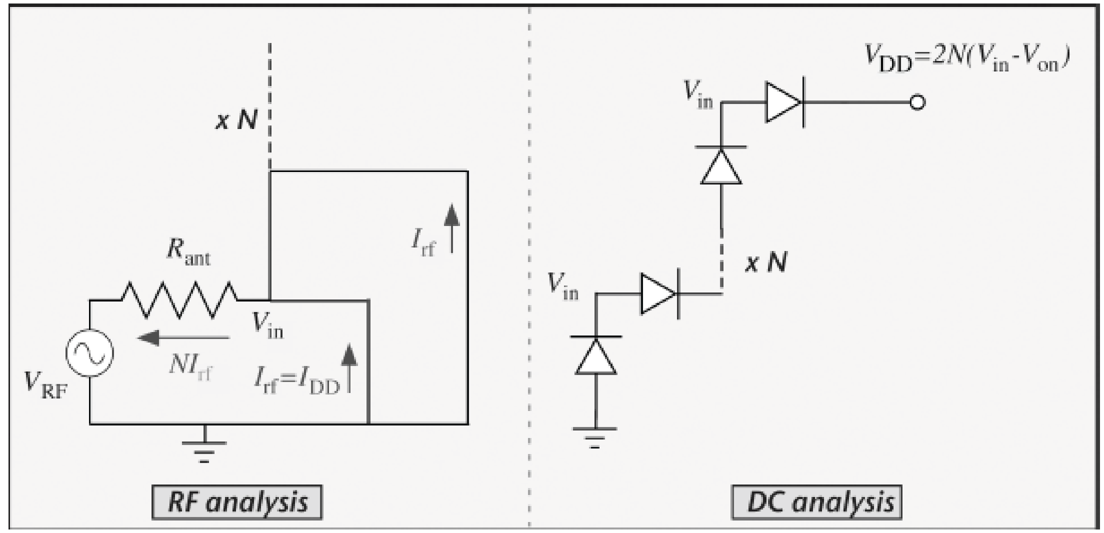


Figure 5.10: Charge Pump Output Analysis. The RF Analysis is Shown at the Time When Vertical Diodes are on; the Horizontal Diodes Produce a Different Topology but the Same Result.

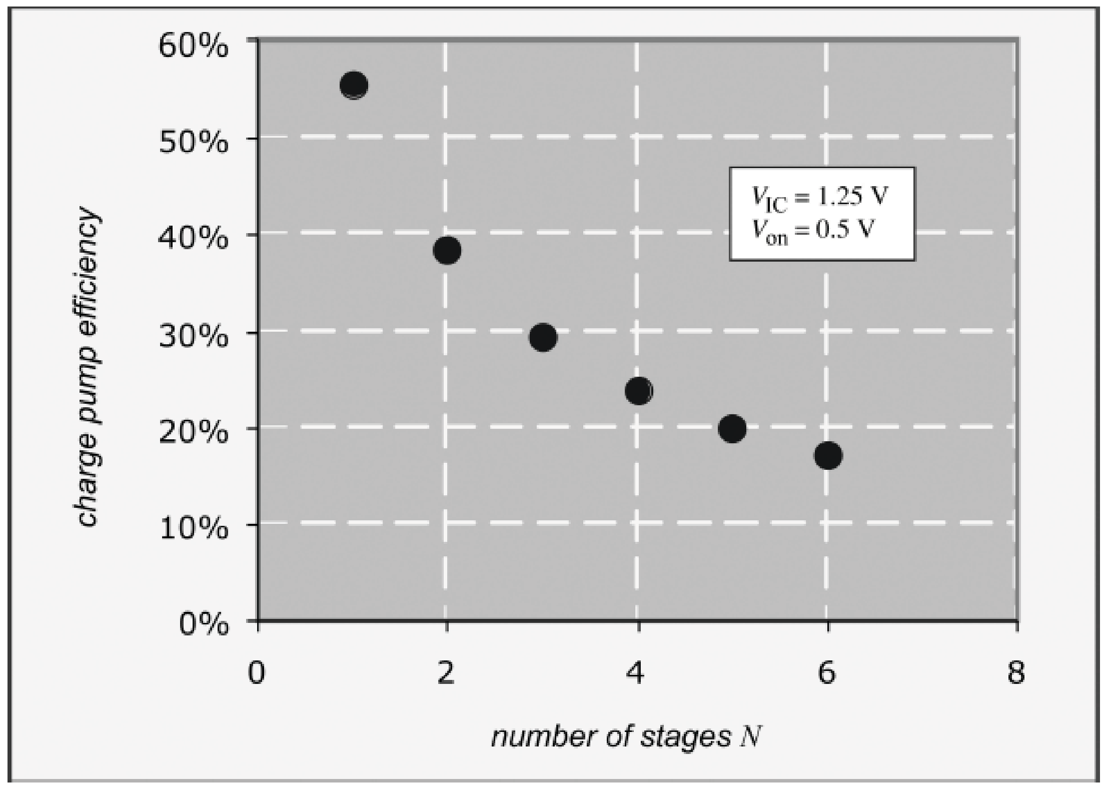


Figure 5.11: Power Efficiency vs. Number of Charge Pump Stages from Equation (5.9).

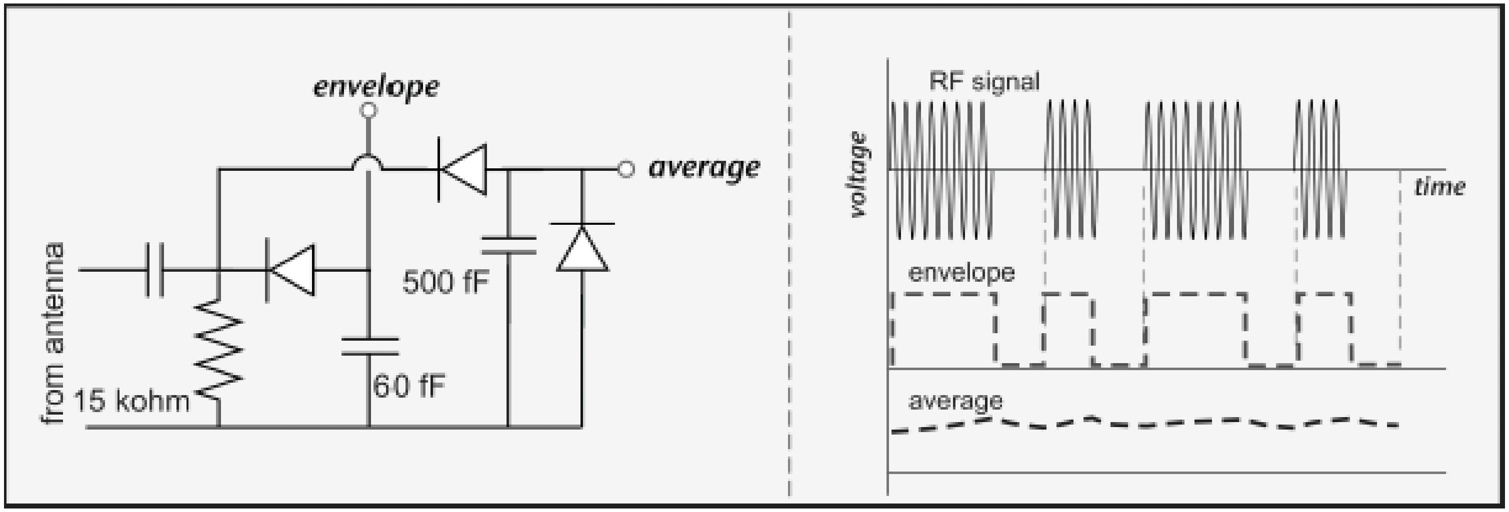


Figure 5.13: Circuit for Extracting RF Envelope and Average Power from Incoming RF Signal; After Curty et al.

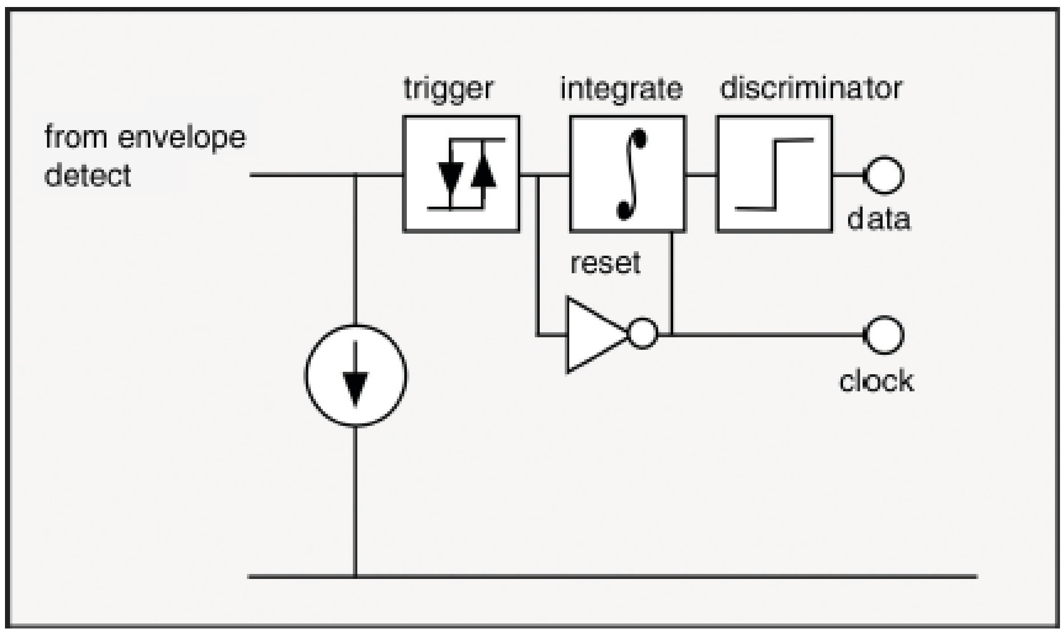


Figure 5.14: Simple Demodulation Circuit for Pulse-interval-encoded Data; After Karthaus and Fischer.

Talking Back

Passive tags use modulation of the power scattered by the tag antenna to reply to the reader. In our earlier discussions of backscatter modulation, we imagined a very simple scheme in which the IC simply interrupts current flow through the antenna to modulate the scattered power (see for example Figure 3.15). Let's take a closer look at how one might modulate the behavior of the antenna and what the consequences are. The three questions we need to address are:

- How much scattered power can we send back to the reader?
- What effect do we have on the power absorbed by the (IC) load?
- How hard is it to implement a given scheme?

Let us first examine the limiting cases of the loads that can be presented to the antenna. These are shown schematically in Figure 5.15. Note that in this and subsequent diagrams, we show an antenna connected to a ground node, which is defined to be at zero voltage. In practice, most tag antennas are symmetric and there is no easy way to define a true "zero" voltage, but the principles are the same, and it is much easier to discuss the problem in this *single-ended* configuration, rather than the actual *balanced* or *differential* connection.

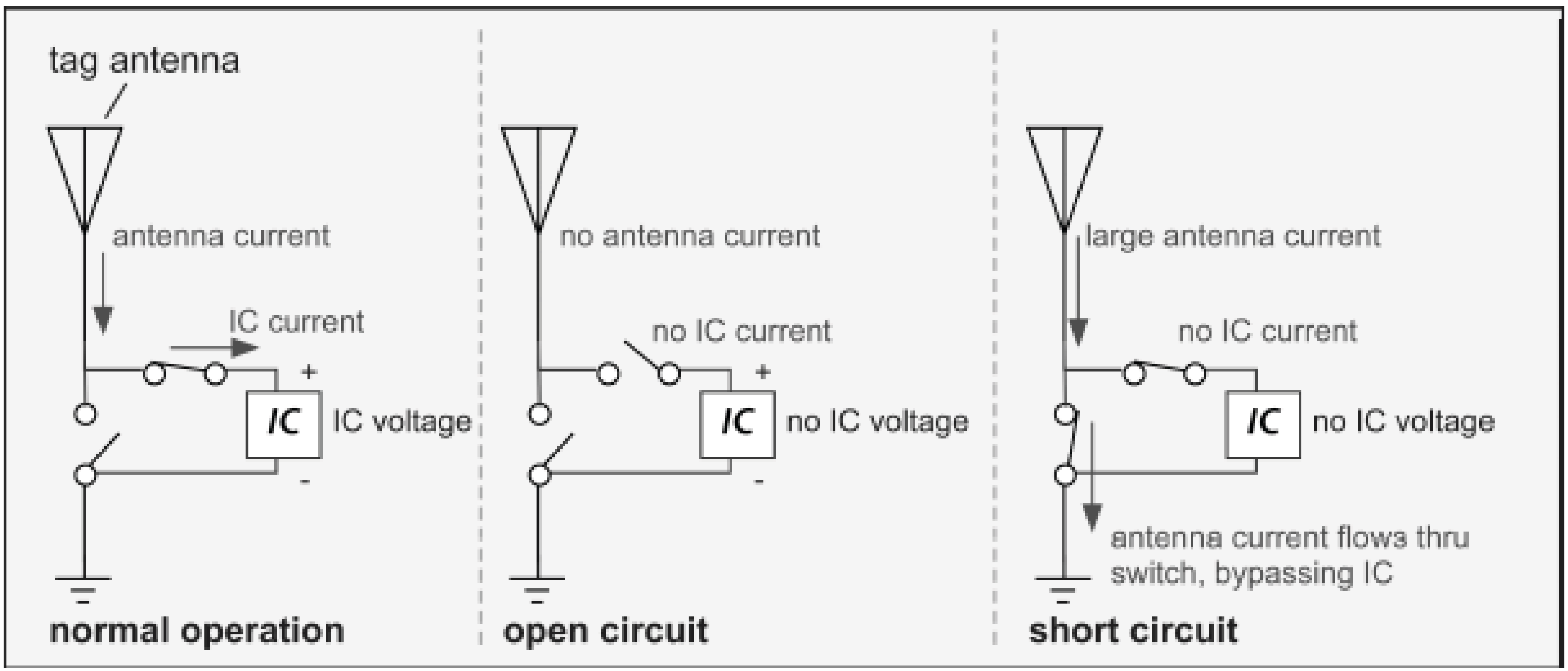


Figure 5.15: Elements of Simple Backscatter Modulation Schemes. Single-ended Antenna Connections are Shown for Simplicity.

Tag IC Overall Design Challenges

Now that we've touched on the problems presented by the interface to the physical world, let us turn our attention to the logic, memory, and supporting systems that make the tag responsive to its environment. A rough functional layout of a typical passive tag IC is depicted in Figure 5.23. Around half the chip area is taken up by the logic needed to implement the relevant protocol: about 50 000 transistors for an 18000-6C (EPCglobal Class 1 Generation 2) IC.

We've looked at the key RF-related challenges in Sections 5.2–5.4 above. The remainder of the chip operates at baseband frequencies and is generally similar to conventional mixed-signal design. However, there are some special challenges peculiar to the RFID world.

The first challenge is, of course, that of cost. The cost of a chip is dominated by its size if yield is reasonably good. Modern IC manufacturing facilities use 200-mm- or 300-mm-diameter wafers. A standard 200-mm-diameter silicon wafer offers a useful area of about 30 000 square millimeters. (This is a bit less than the total surface area: the region within about 3 mm of the wafer edge is usually not useful for processing.) If a single IC has a useful area of around 1 mm2, we can get about 22 000 chips from a wafer assuming that 90% of the chips are good (that is, the yield is 90%). In small volumes, it costs about $1000 to purchase a processed wafer, so the cost of these ICs would be roughly $0.05 per chip. The use of 300-mm wafers increases the initial cost for masks, but in high volume the ongoing cost is reduced by 30–40% vs. 200-mm wafer. The actual numbers are influenced by such commercial issues as volume pricing—I don't pay $1000/wafer if I buy several hundred wafers—but it should be apparent that at 1 square millimeter, the chip cost is a substantial fraction of the $0.05 tag cost goal promulgated by such organizations as EPCglobal. It is imperative to keep the chip as small as possible to minimize IC cost.

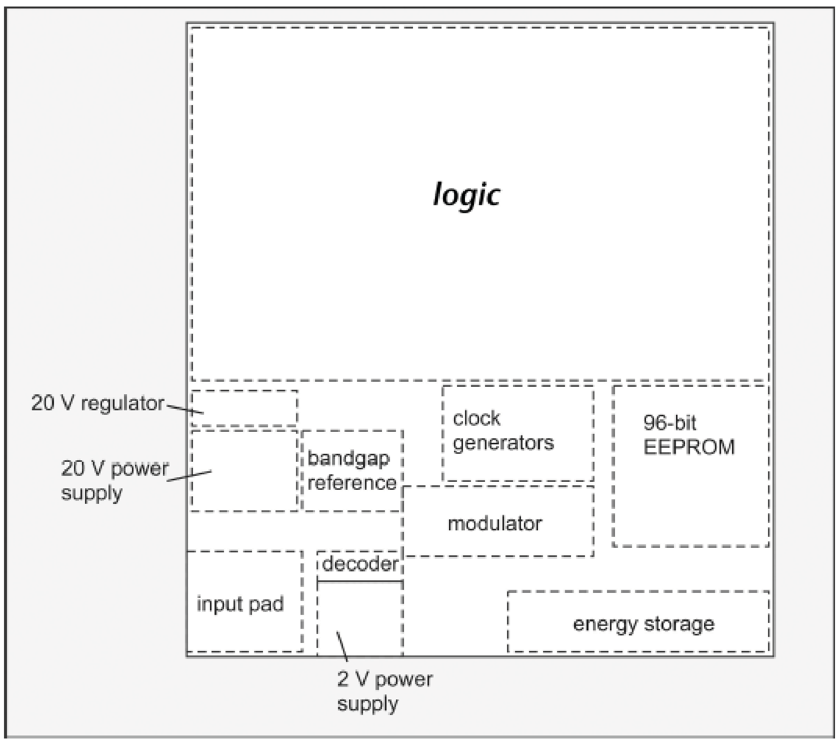


Figure 5.23: Functional Layout of a Tag IC (After Stewart).

iClass Security

The HID iClass family of 13.56 Mhz Contactless readers and cards was introduced over a decade ago with the primary goal of eliminating some of the security concerns that existed with the older 125Khz Proximity technology. The state-of-the-art iClass technology supported new features such as mutual authentication and Triple DES encryption to improve security and reduce the possibility of card duplication.

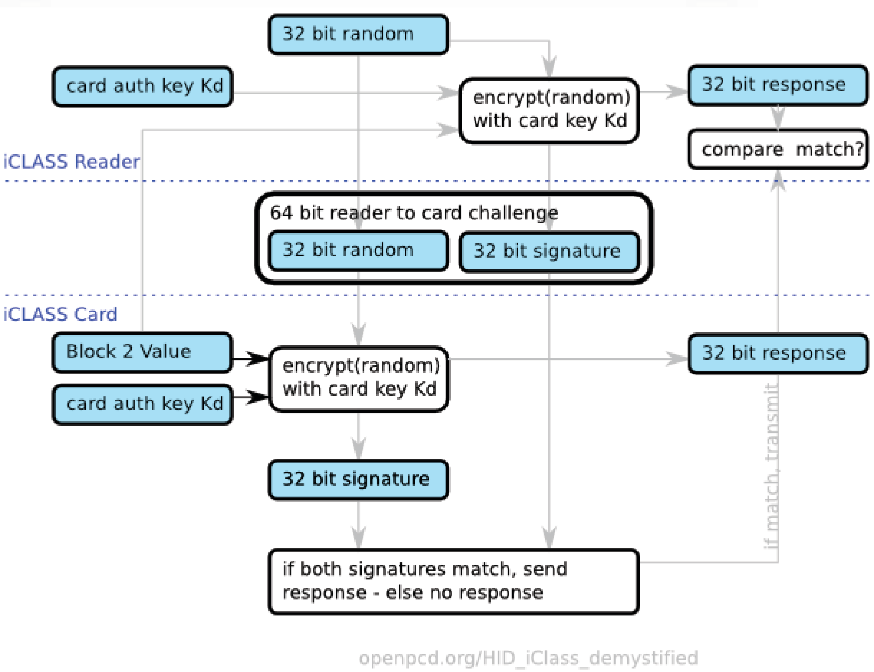
The contactless cards themselves utilize an embedded chip technology called "PicoPass" from a French company by the name of Inside Secure http://www.insidesecure.com/ . These chips basically consist of a small EEPROM memory and a simple state machine controller that is used to interact with a card reader using the ISO 14443B and ISO 15693 protocols.

All data stored on iClass cards is secured by Authentication Keys. A Key is basically a password used to protect data from being read or changed without authorization. The iClass cards and readers use 64-bit keys (56 key bits plus 8 parity bits). One authentication key is used to protect each of the card’s Application Areas. Two encryption keys are used to support TDES encryption of the transferred data.

Since its introduction, numerous articles have been written by HID and other security industry experts who have all described the technology as "Extremely Secure" and "Difficult to Clone". Those kinds of words are usually interpreted by the hacking community as an open challenge to explore the technology and to identify and exploit any vulnerabilities that are found to exist. As a result, within the last year at

OpenPCD.org

http://www.openpcd.org/HID_iClass_demystified



27TH CHAOS COMMUNICATION CONGRESS IN BERLIN, DECEMBER 2010

Heart of Darkness - exploring the uncharted backwaters of HID iCLASS™ security

Milosch Meriac, *meriac@OpenPCD.de*

***Abstract*—This paper provides detailed information on *iCLASS*™ reader and key security. It explains the security problems found without revealing the extracted secret keys (DES authentication Key and the 3DES data encryption key for *iCLASS*™ Standard Security cards).**

The chosen approach of not releasing the encryption and authentication keys gives iCLASS vendors and customers an important headstart to update readers and cards to High Security mode in order to stop attackers from forging, reading and cloning iCLASS Standard Security cards.

This paper also explains, how Standard Security and High Security keys were extracted from a RW400 reader without leaving visible traces.

One of the biggest *don't*s in card security is to design a card security system which allows copying cards without forcing the attacker to use a card emulator. Out of no apparent reason this implementation flaw exists for HIDs iCLASS cards: Knowing the authentication key results in beeing able to copy the cards - decrypting 3DES encrypted content is not necessary for that.

IX. Recommendations

- Standard Security Mode is dead[19]. Switch immediately to High Security by asking your local HID vendor for programming cards that will upgrade your Standard Security system to High Security and rotate your existing cards to the new keys at a trusted location only. **Make sure that your vendor tells you the new High Security key.**

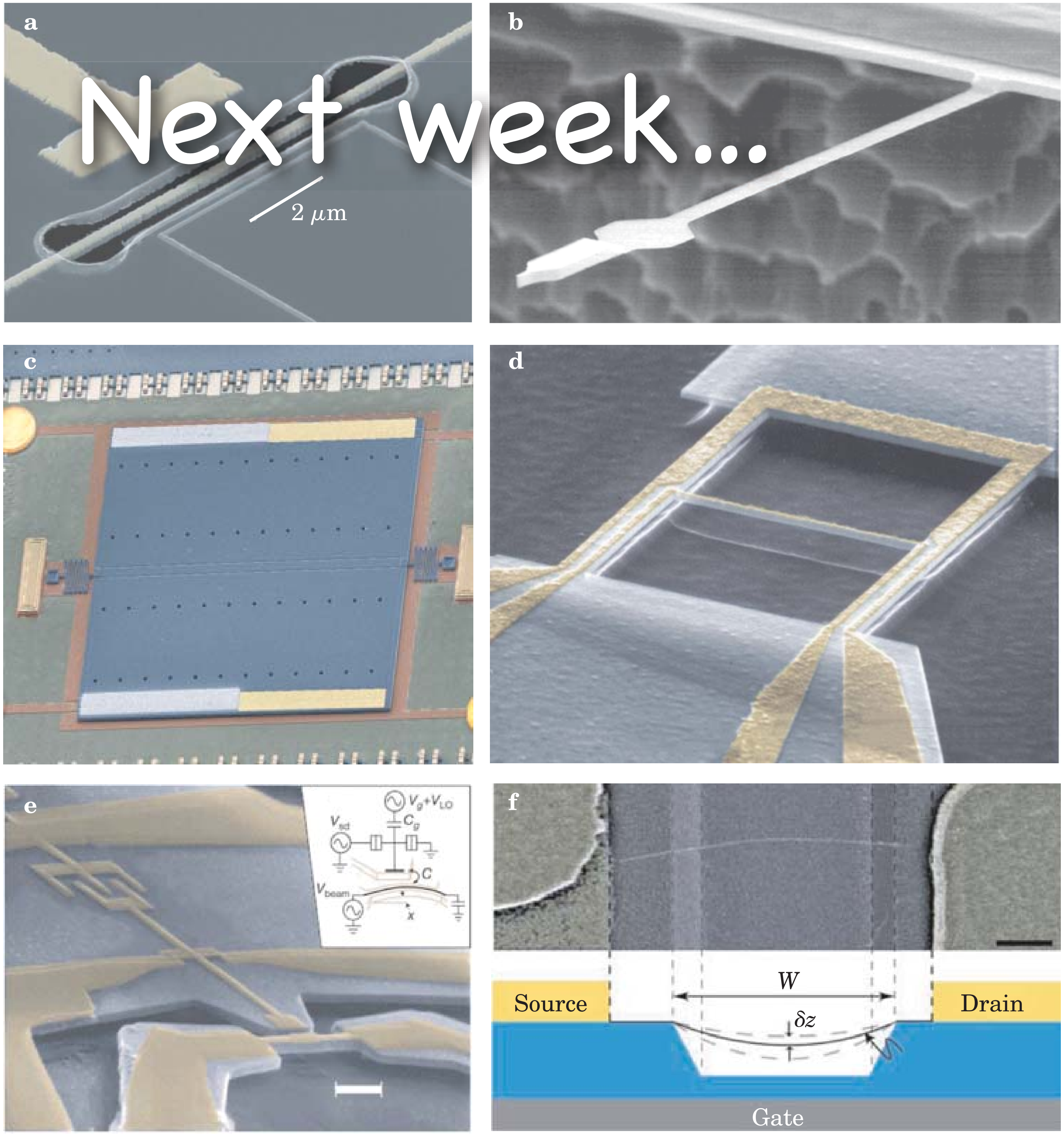


Figure 1. Nanoelectromechanical devices. **(a)** A 20-MHz nanomechanical resonator capacitively coupled to a single-electron transistor (Keith Schwab, Laboratory for Physical Sciences).[11] **(b)** An ultrasensitive magnetic force detector that has been used to detect a single electron spin (Dan Rugar, IBM).[3] **(c)** A torsional resonator used to study Casimir forces and look for possible corrections to Newtonian gravitation at short length scales (Ricardo Decca, Indiana University–Purdue University Indianapolis). **(d)** A parametric radio-frequency mechanical amplifier that provides a thousandfold boost of signal displacements at 17 MHz (Michael Roukes, Caltech). **(e)** A 116-MHz nanomechanical resonator coupled to a single-electron transistor (Andrew Cleland, University of California, Santa Barbara).[10] **(f)** A tunable carbon nanotube resonator operating at 3–300 MHz (Paul McEuen, Cornell University).[14]