RFID

Identification systems (IDFS)

Department of Control and Telematics
Faculty of Transportation Sciences, CTU in Prague

Discussion

- What is RFID?

RFID

- Radio Frequency Identification (RFID) is a wireless data collection technology to identify physical objects in a variety of fields.

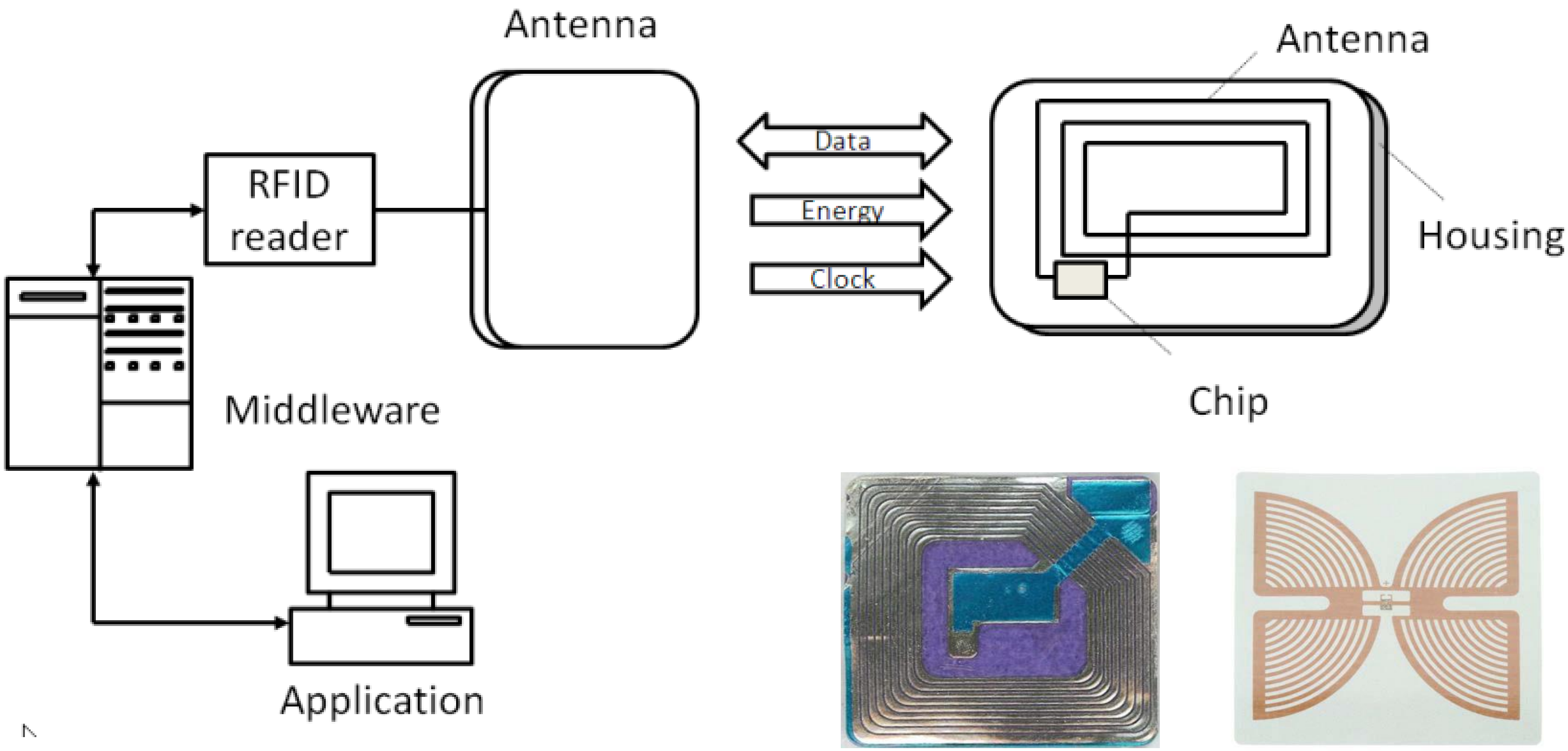
Data storing principle:

- Allows to **store electronic data** (binary) and retrieve them in electronic means.
- It is a successor specially of barcodes systems, follows **same data structure principle**.

Communications principle:

- The RFID is the combination of radio broadcast technology and **radar**
- Radar sends out radio waves for detecting and locating an object by the reflection of the radio waves.

RFID principle – TAG breakdown



Referring to: Finkenzeller (2010)

Figure 3. Basic layout of an RFID data-carrying device, the transponder and other main components of an RFID system

RFID History

- Harry Stockman, "Communication by Means of Reflected Power", published in October 1948, first groundwork for RFID
- D.B. Harris, "Radio transmission systems with **modulatable passive** responder“, published if ~1950
- Robert Freyman "Short-range radio-telemetry for electronic identification using **modulated backscatter**" in 1975.

Use of RFID:

- **EAS** (electronic article surveillance) – around 1960, simple 1bit tags, inductive or microwave
- "Electronic identification system" in 1975, by RCA
- RFID for collection of tolls – Norway 1987, USA 1989
- First open highway electronic tolling system, USA, Oklahoma 1991

Discussion

- Where it is used?

Different application of RFID

- Manufacturing and Supply Chain Tracking
- Goods tracking (Retail)
- Asset Tracking (monitoring the health of animals)
- People Tracking (Travel, Facebook RFID , clothes)
- Health care - Edible RFID Tags
- Automotive industry – anti-theft immobilizers, Smart Plates
- Navigation Systems for the Visually Impaired
- Waste Disposal
- Contactless payments (NFC)
- IFF identification, etc.

http://www.simonsothcott.com/2011/11/what-is-rfid-10-examples-of-rfid.html

Discussion

- Are there any benefits over the barcodes?

Comparison

Compared to Bar Codes

- RFID tags do not require line-of-sight reading
- RFID scanning can be done at greater distances.
- RFID tags can store significantly more information
- RFID unique serial number allows tracking of individual items.
- More expensive than Bar Codes

Compared to OCR

- OCR technology have high density of information and the ease of reading data,
- OCR is more expensive than RFIDs and requires complicated readers

Types of RFID Tags

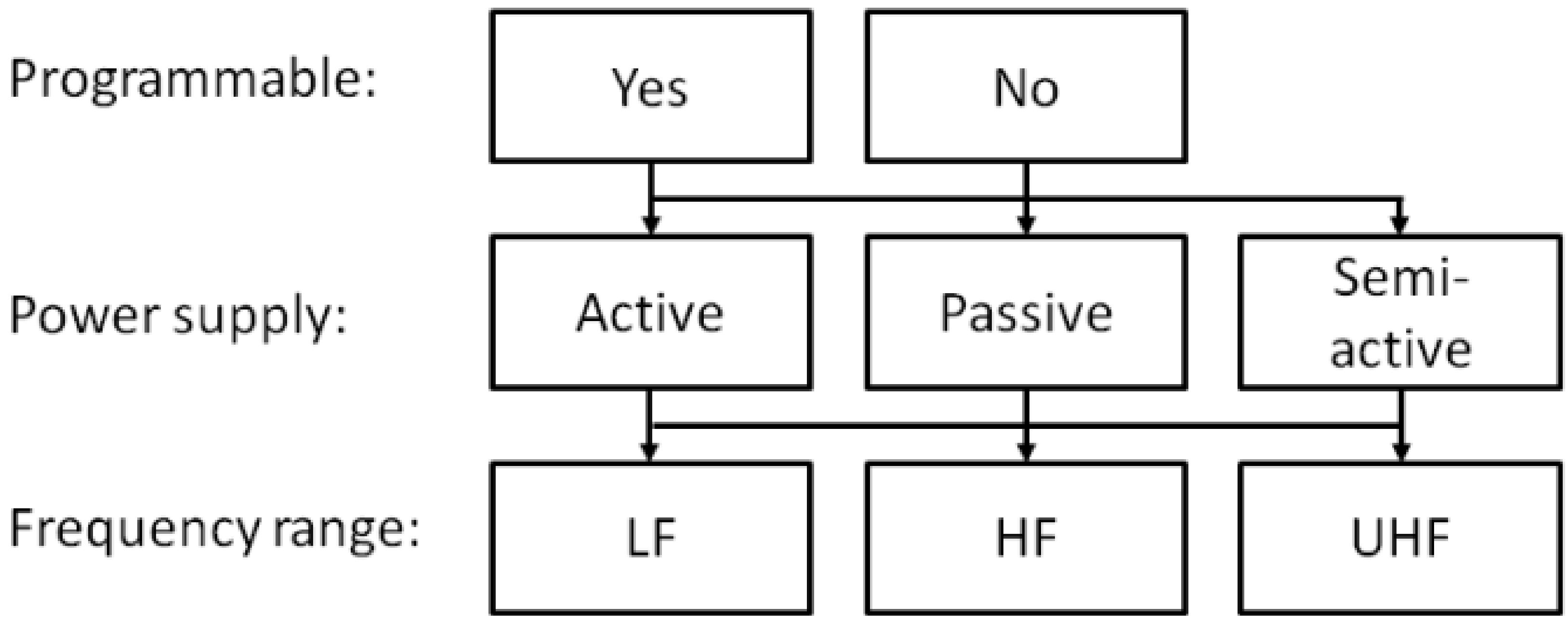
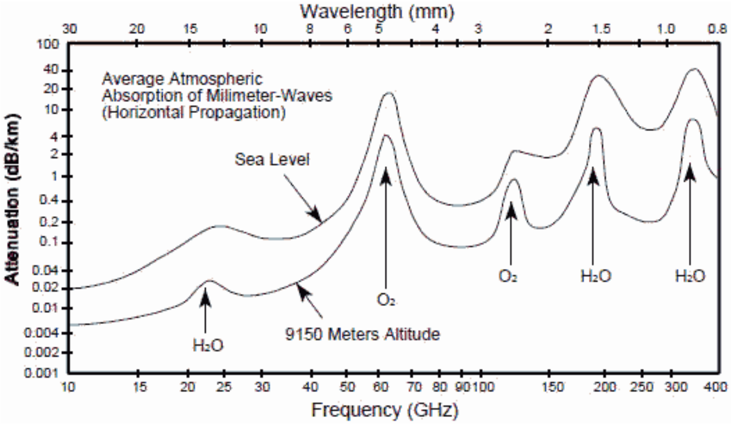


Figure 5. The features of RFID systems

Frequency ranges

- Frequency determining factors:
  - material of the object being tagged
  - the read range required



- tags are designed to operate in the
  - **low frequency** (LF, frequencies from 30–300 KHz, most popular for access control, but also for animal and human ID)
  - **high frequency** (HF, from 3–30 MHz, widely used for smart cards and asset tracking and supply management)
  - **ultra-high frequency** (UHF, from 30–3000 MHz, due to wide frequency ranges ideal for tracking large and expensive objects, also the design for the length of life.)

Power supply?

- A tag needs energy/power to be able to send and receive data

- Classification according to how tags obtain power to operate:
  - **passive**, (have no power of their own, only work when supplied with the radio signal from the reader)
  - **semi-passive** (battery assisted tags, tag is able to function independently, do not have active transmitters) and
  - **active**. (have their own power source (battery or an active transmitter). Read-and-write range is potentially greater.

Programmable?

- **Read-only tags**
  - contain a **non-changeable programmed identifier** that remains during the chip’s life.
  - generally inexpensive but cannot be reused and can only store a limited amount of data.
- **Read-write tags**
  - more sophisticated because of the possibility they offer to reprogramme the tag with new information,
  - can be erased and reused, thereby significantly reducing costs while contributing to environmental sustainability.
  - can store and process information locally, valuable when dealing with high-volume, complex supply-chain applications.

Comparison of tags

Table 1. Comparison of some of the typical features of passive vs active RFID

Feature	Passive	Active
Size and weight	Small (or thin)	Large
Cost	4 €cents to <1€	3€ to a <100€
Life	Virtually unlimited	3 to 7 years
Range	Up to 30 metres	Up to 30 metres
Reliability	Excellent	Good
Sensor input	Little or none	Any
Can emit continuous signal	No	Yes
Area monitoring/geofencing	Rarely	Yes
Multi-tag reading	Fair or none	Excellent (e.g., thousands)
Location using a beam	Yes, but only short distance	Yes, at long distance
High-speed reading	Fair	Excellent
Data retention	Small to medium (e.g., 1 Kbit)	Medium to high (e.g., 1 Mbit)
Very slow signal power	No	Yes – no need to get the signal and back because semi-active and fully active tags emit their own signal and the battery boosts it
Security features of signal and processing	Limited	Excellent
Event signalling	No	Yes
Electronic manifest	No	Yes
Data logging	No	Yes

Source: Das & Harrop (2010)

RFID Data

Identification of RFID chips (EPCglobal Tag Data Standard Version 1.6)

- RFID chips contains 96 or 64 bit unique number

  -> **EPC** = Electronic Product Code

- EPC has 4 main parts:
  - Header – defining the length, type and structure of the code
  - EPC manager number – identifying the company
  - Object class – defining the actual object
  - Serial number – identification of actual object within the given type

Header	EPC Manager Number	Object Class	Serial Number

Uses of EPC

- As URI - preferred way to denote a specific physical object example: urn:epc:id:prefix

The formal grammar for the EPC URI is as follows:

```
EPC-URI ::= SGTIN-URI | SSCC-URI | SGLN-URI
          | GRAI-URI | GIAI-URI | GSRN-URI | GDTI-URI
          | GID-URI | DOD-URI | ADI-URI
```

- Serialized Global Trade Item Number (SGTIN)

General syntax:

urn:epc:id:sgtin:*CompanyPrefix.ItemReference.SerialNumber*

Example:

`urn:epc:id:sgtin:0614141.112345.400`

Grammar:

```
SGTIN-URI ::= "urn:epc:id:sgtin:" SGTINURIBody
SGTINURIBody ::= 2*(PaddedNumericComponent ".")
GS3A3Component
```

- Serial Shipping Container Code (SSCC)

ftp://epsfiles.intermec.com/eps_files/eps_man/937-023-002/Content/RFID_Tag_Info/

Discussion

- Issues with using RFID?

Implication of using RFID technology

Privacy

- the concern is that information gleaned from privacy attack may then be used more widely for impersonation or identity **theft**.
- The owner of the RFID interrogator would then be privy to information about the user's **habits**, which, in itself, would be a **breach of** the user's **privacy**

Security

- Companies need to protect their data by ensuring that the RFID technology adopt and supports corporate security policies.
- Companies need to be aware of the security risks, such as **profiling**, eavesdropping , denial of service attacks and inventory jamming.

low frequency (LF, frequencies from 30–300 KHz)

high frequency (HF, from 30–300 MHz)

ultra-high frequency (UHF, from 300–3000 MHz)

COMMUNICATIONS CONCEPTS

Communication over the air interface

Low-and middle frequency ("LF, MF") tags,

- operate in range 30 kHz to 3 MHz. Typically **125 kHz or 134,2 kHz.**
- Wide spread, can be used in bad environmental conditions.
- for short-range uses, like animal identification and anti-theft systems, such as RFID-embedded automobile keys.
- large antenna (solenoid) = cost and size problem

High frequency ("HF") tags.

- operate in range 3 MHz to 30 MHz. Typically at **13.56 MHz.**
- Have higher communication speed (data rate).
- Can be used in bad environmental conditions, but water affects reading range. Read range to 1m
- Used in smart cards in libraries (books), luggage tagging,

Communication over the air interface

Ultra-High Frequency ("UHF") tags

- operate in range 300 MHz to 3 GHz. Typically at **915 MHz (USA) / 868 MHz (Europe) for passive tags. For active also 2,4 GHz**
- Have higher communication speed (data rate)
- High reading range of 3m / 10m (in case of 2.4 GHz)
- Susceptible for metal presence, can not be used in humid / water environments.

Microwave Frequency ("SHF, EHF") tags

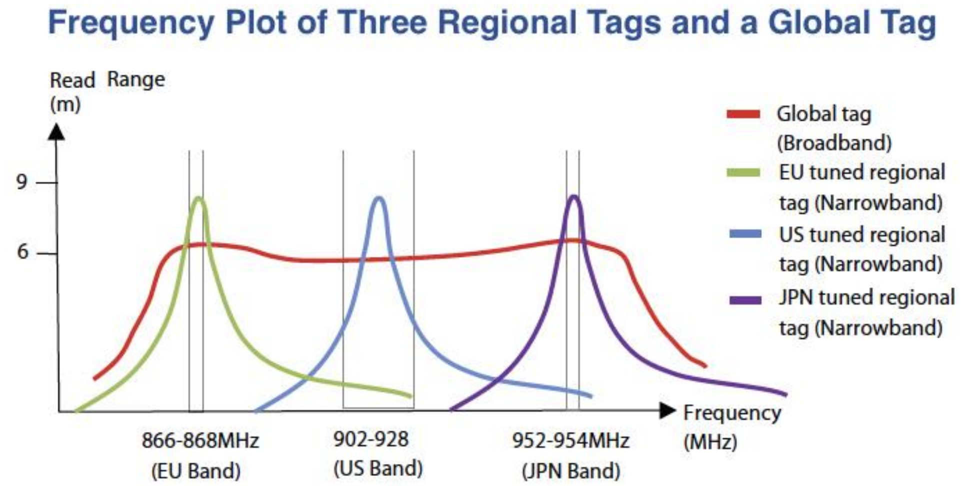
- operate in range 3 GHz to 300 GHz. Typically at **5,9 GHz (USA) / 5,8 GHz (Europe)**
- Have advantages and disadvantages of the above but with greater effect

Communication over the air interface

Frequency choice affects

- Reading range and reading speed
- Tag size (lower frequency = bigger antenna)
- Antenna type, solenoid vs. dipole
- Environmental ruggedness (lower frequency = better)
- Price (higher frequency = higher price)

- Interoperability – in UHF

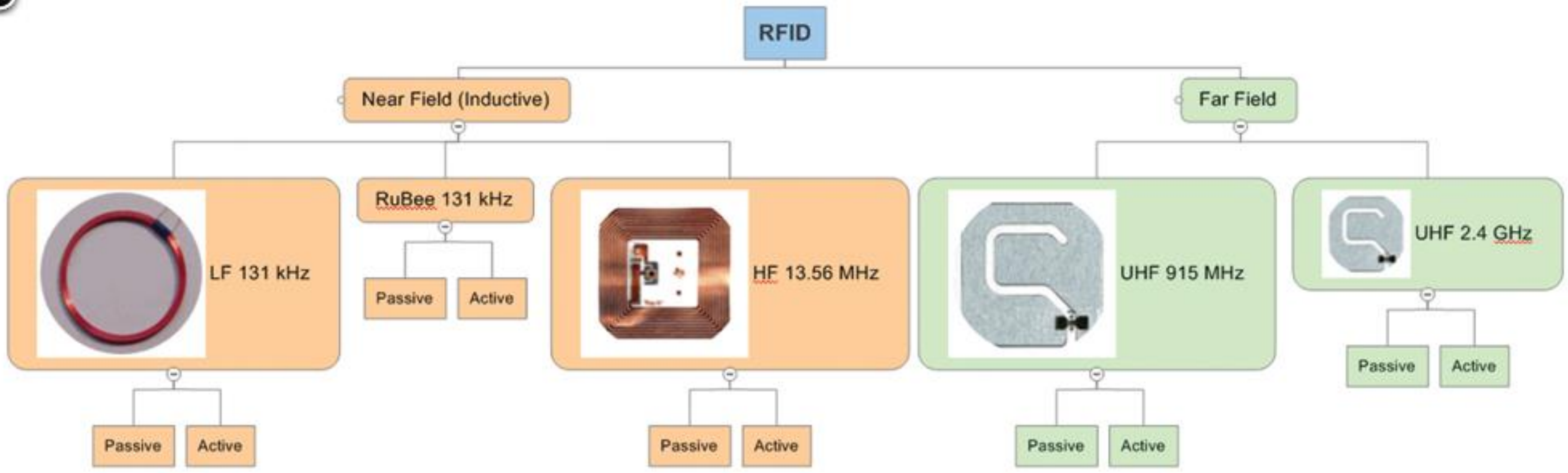


Passive RFID Standards (freq. and characteristics)

Passive RFID Standards	**UHF**	**HF**
Protocols	EPC Gen 2	ISO 15693
	(ISO 18000-6C)	ISO 14443
RF Transmission	Propagating	Electromagnetic
	Back Scatter	**Ind. Coupling**
Frequency	860-960 MHz	13.56 MHz
Read Ranges	3-5 meters+	1 meter 0.1 meter
Reader Cost	500-$2000	100-$1000
Tag Cost	~0.10-$0.20	0.20-$0.50
Memory Storage	96 bits to 1 Kbits	256 bits to 8 Kbytes

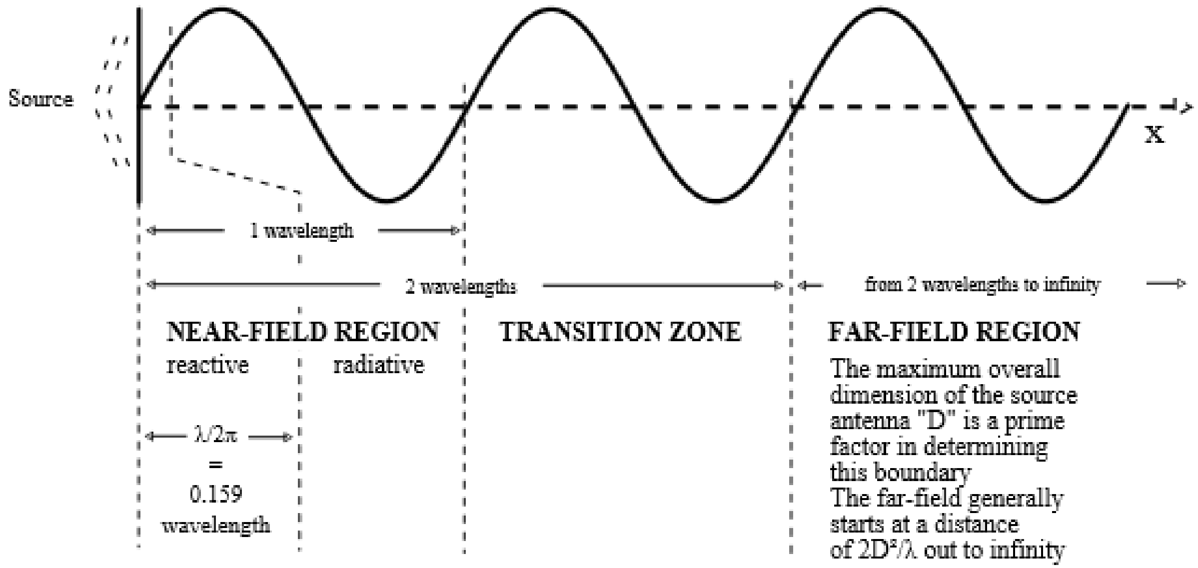
Communication over the air interface

- Generic frequencies for RFID:
  - Inductive coupling LF 125 - 134 kHz, HF 13.56 MHz, UHF 400, (in reactive near field)
  - Backscatter 860 – 960 MHz, 2.45 GHz, 5.8 GHz (in far field)



Far versus near field

- **far-field** = "normal" electromagnetic radiation. The power of this radiation decreases as the square of distance from the antenna.
- **near-field**, Absorption of radiation in the reactive part affect the load on the transmitter. Magnetic induction can be seen as a very simple model of this type of near-field electromagnetic interaction.



Wiki, and: http://www.drillingcontractor.org/the-abcs-of-rfid-physics-oilfield-usage-14030

Example of reactive NEAR field read ranges

- How far ranges reactive **near field**?

Example 1 (900 MHz)

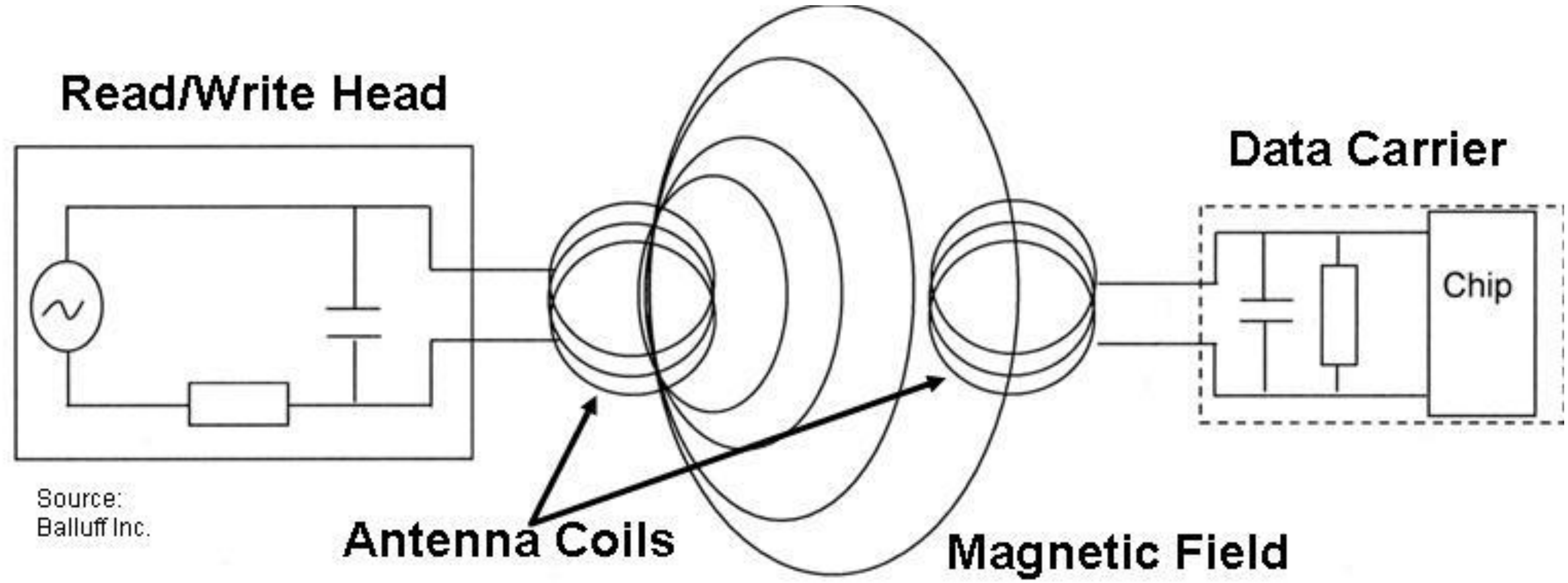
- At 900 MHz, the wavelength is: $\lambda = 300/f_{MHz} = 300/900 = 0.333$ m
- near field is calculated as: $\lambda/2\pi = 0.159\lambda = 0.159(0.333) =$ **0.053 m**
- Read ranges usually extend somewhat beyond this point.

Example 2 (13.56 MHz)

- NFC uses the near field as the read range,
- The NFC frequency is 13.56 MHz, wavelength of $\lambda = 300/f_{MHz}$
- $300/13.56 = 22.1$ m, near field is within: $\lambda/2\pi = 0.159\lambda =$ **3,5 m**
- Because less power is used, the actual read range is rarely greater than a foot.

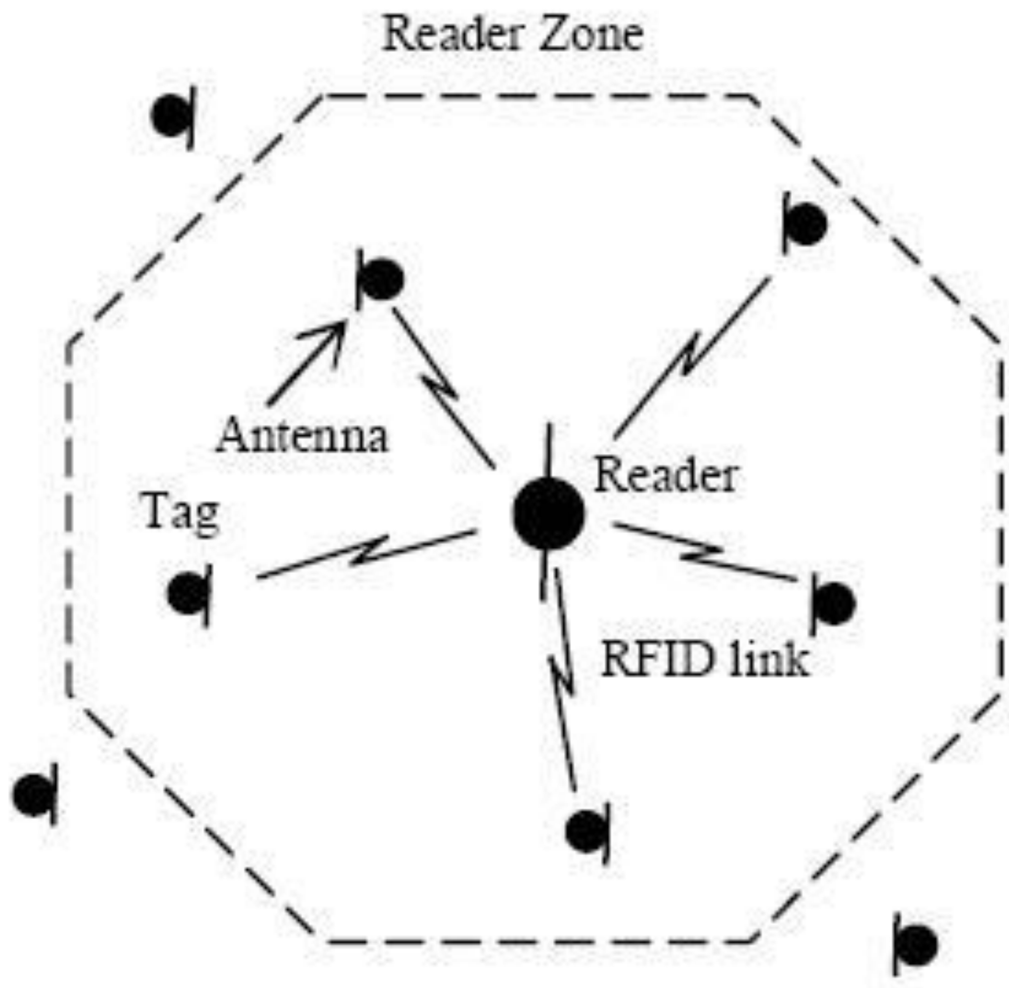
Communication over the air interface

- Near field communication over inductive coupling



- Both reader and tag antennas are usually loops serving as the primary and secondary of a transformer.

RFID communication – anti-collision mechanisms



Communication over the air interface

Communication with the TAG – different principles

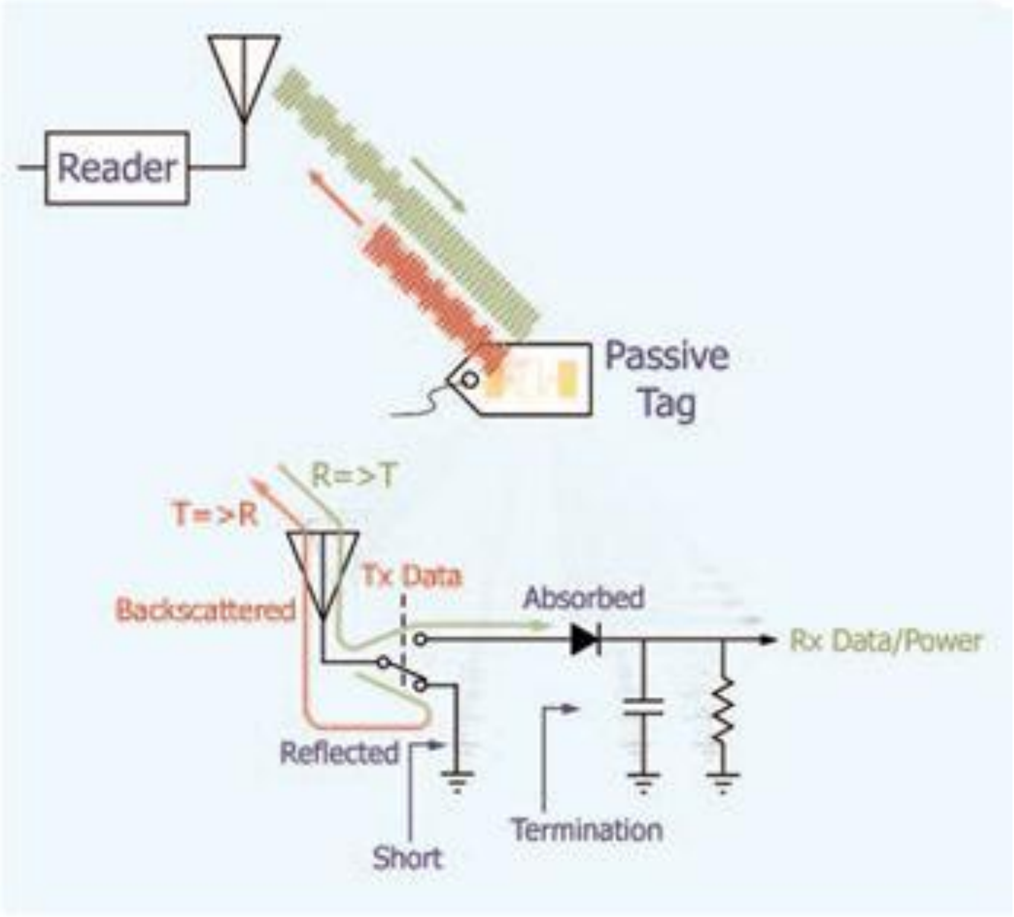
- RTF (reader talks first) – silent even if illuminated by reader – waits for a “question”.
- TTF (tag talks first) – for passive and semi passive tags it means “talking” as soon as it is illuminated. For active tags automatically talks even if no reader is present.

anti-collision mechanisms:

- Reader side
  - FDMA / TDMA
- Tag side
  - Aloha (in timeslots)
  - Tree walking

- Next lecture

Backscatter communication



Communication over the air interface

Link Coding

- For digital data transport line coding is often used.
- Line coding consists of representing the digital signal to be transported, by an amplitude- and time-discrete signal, that is optimally tuned for the specific properties of the physical channel (and of the receiving equipment).
- The waveform pattern of voltage or current used to represent the 1s and 0s of a digital signal on a transmission link is called line encoding.

- **NRZ, Manchester, RZ, Miller, PWM**

Communication over the air interface

Reader to tag

- The information (from reader to tag) is conveyed through changes in amplitude (ASK), phase (PSK) or frequency (FSK) of the carrier signal.
- Another technique is Pulse Width Modulation (PWM) in which the information is conveyed through variations of the width of pulse.

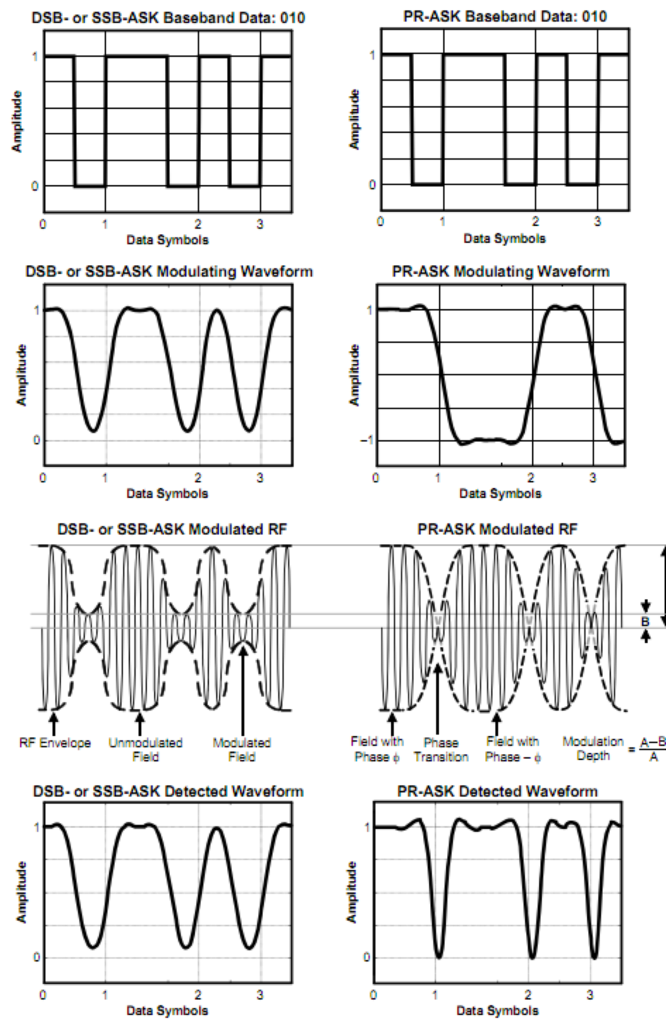


Figure H.1 – Interrogator-to-Tag modulation

Tag to reader

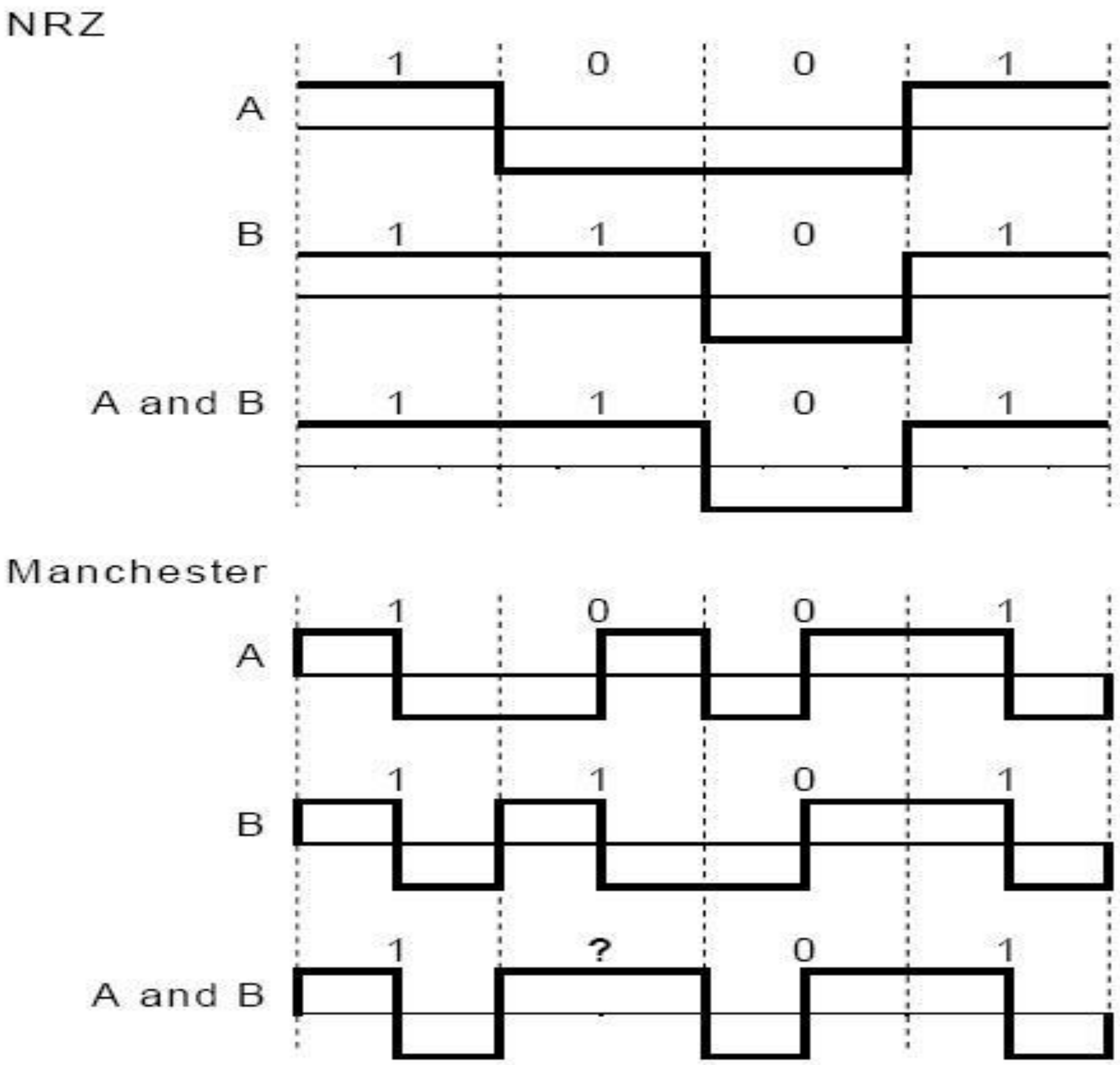
- RFID applications use the Backscatter Modulation technique whether it is ASK or PSK in transferring data from the tag (transponder) to the reader (interrogator)

Collision Detection

- Anti-collision methods require <u>the ability to detect collision</u>
- Collision detection <u>relies on coding scheme</u>
- When simultaneously transmitted signals coded by certain schemes add, they can not be resolved

- Manchester and other transition codes <u>inherently allow this means of collision detection</u>
- NRZ and related level codes <u>DO NOT allow this means of collision detection</u>

Collision Detection

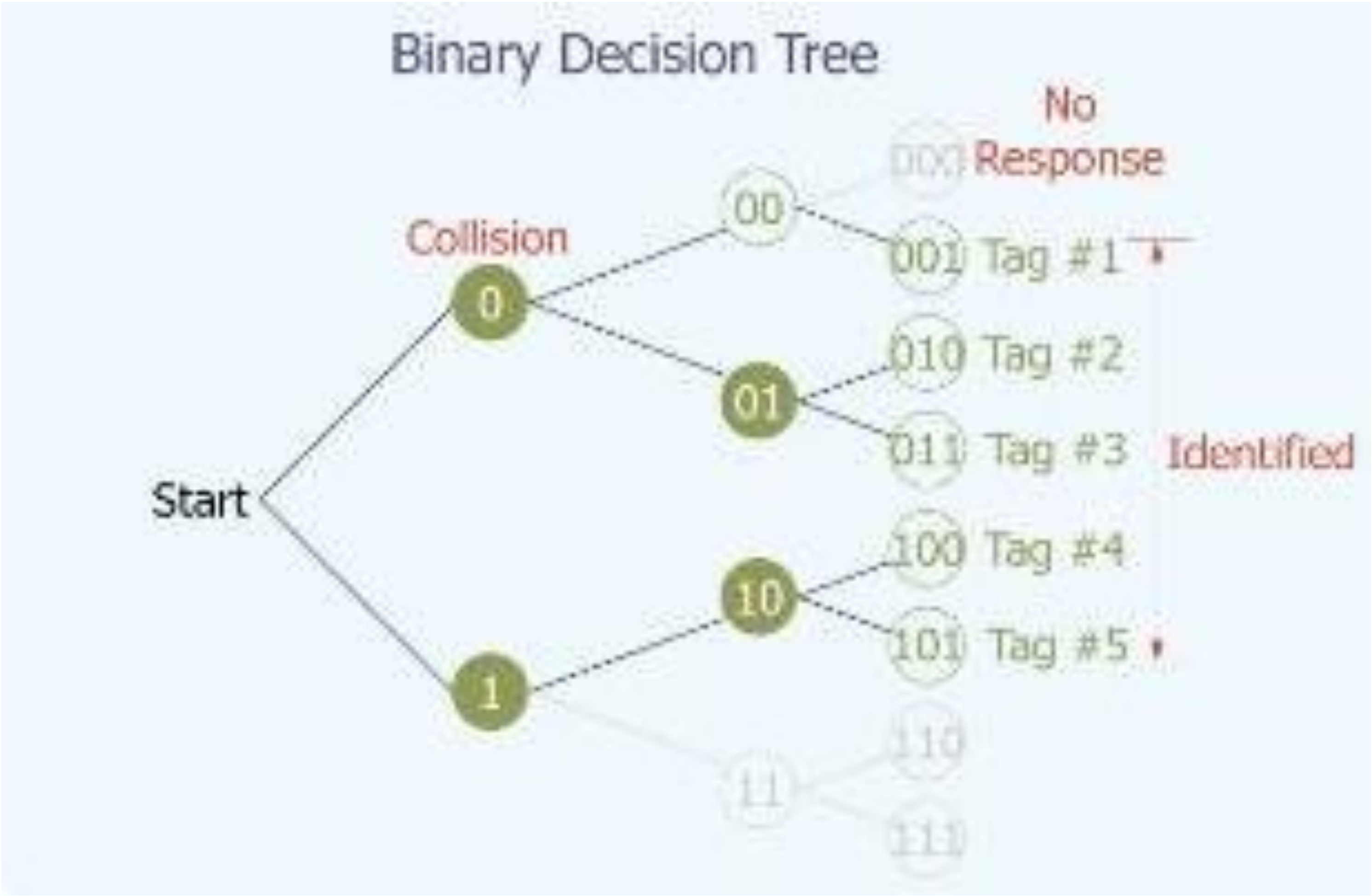


Collision Detection

- Other methods rely on modulation schemes
- Through FSK modulation in tag to reader transmission, readers can detect “woobles” when multiple tag responds simultaneously

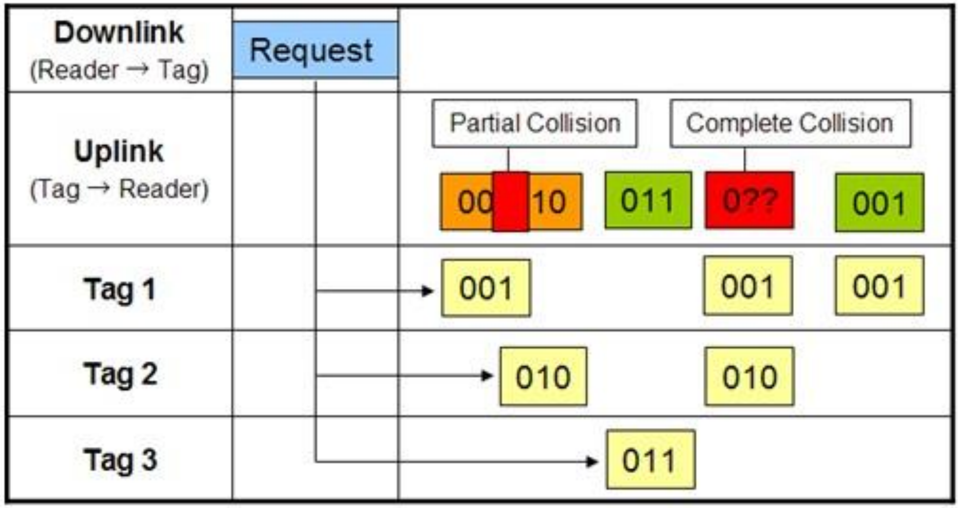
anti-collision mechanisms:

- Reader side
  - FDMA / TDMA
- Tag side
  - Aloha (in timeslots)
  - Tree walking

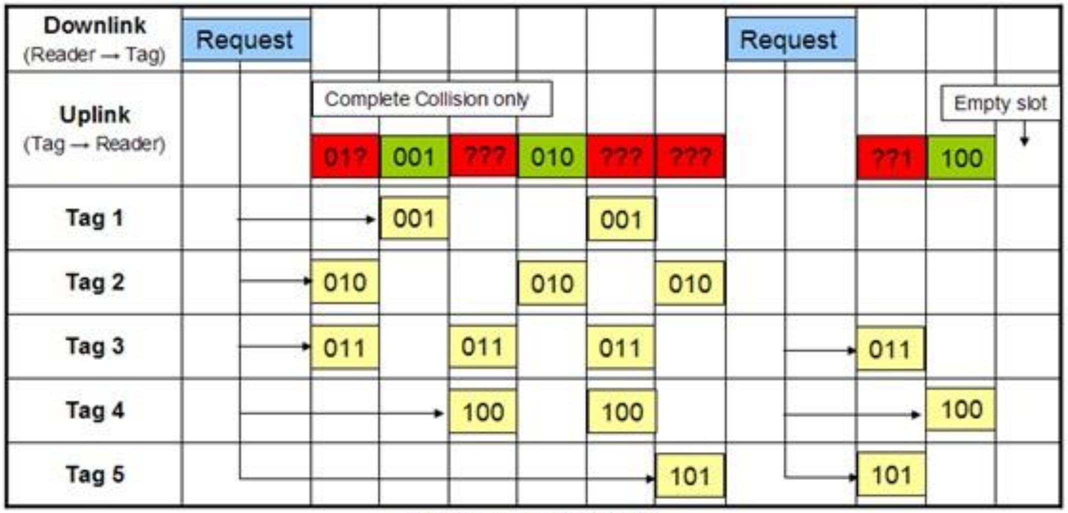


Binary Decision Tree
No
Response
Collision
Start
0
1
00
01
10
11
001
Tag #1
010
Tag #2
011
Tag #3
100
Tag #4
101
Tag #5
Identified
110
111

ALOHA

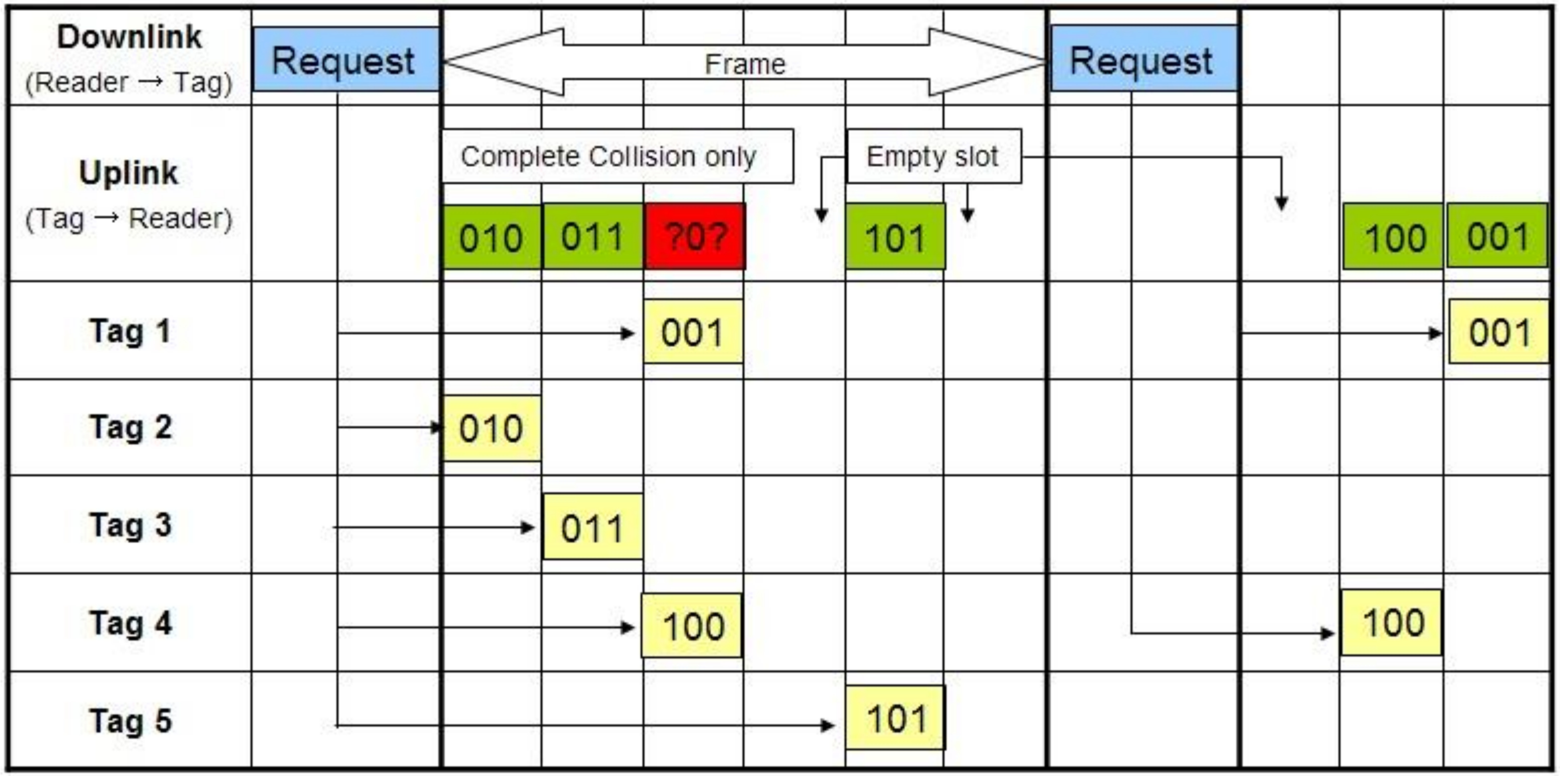


(a) (Pure) ALOHA



(b) Slotted ALOHA

framed slotted ALOHA



PASSIVE RFID TAG / TRANSPONDER

RFID

Interrogator to Transponder	
Carrier Frequency fc:	13.56MHz +/- 7kHz
Modulation Type and Index:	ASK 10%
Data Rate:	212kbps (fc/64) / 106kbps (fc/128)
Bit Representation:	NRZ
Transponder to Interrogator	
Applied Magnetic Field Modulation:	Load Switching
Subcarrier Frequency:	847.5kHz
Subcarrier Modulation Type:	BPSK
Data Rate:	212kbps (fc/64) / 106kbps (fc/128)
Bit Representation:	NRZ

Passive Tags

- Passive tags have no
  - On-tag power source - they make use of the power received from the incoming RF signal to generate their own supply voltage
  - On-tag transmitter
- Passive tags have ranges of less than 10 meters
- Low cost

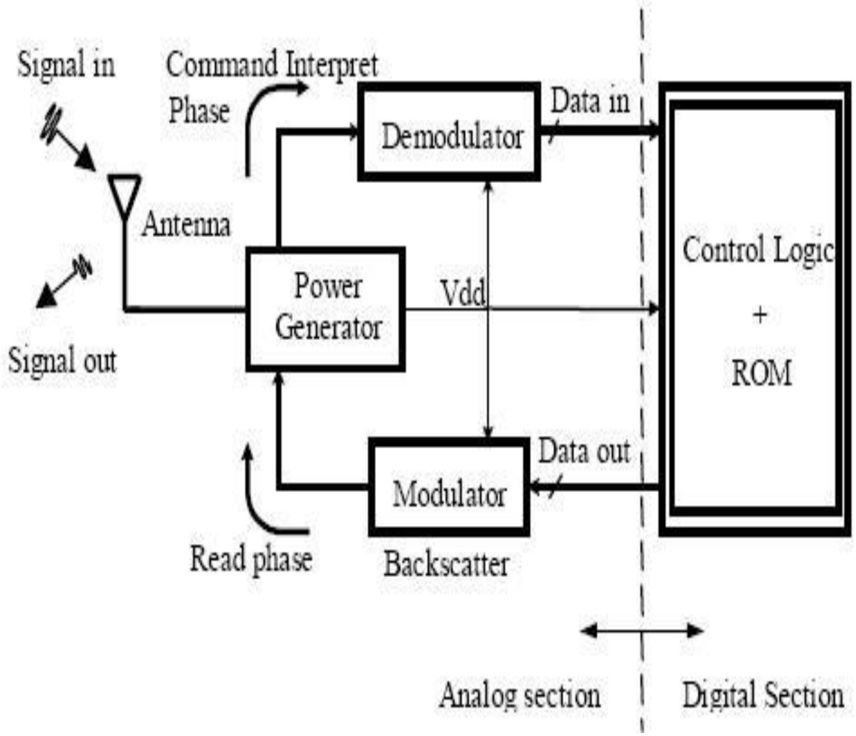
Passive Tags

Main concerns

- Power consumption – <u>relies on electromagnetic fields for power</u>, energy is limited
- Size – directly affects cost; the <u>more silicon is used, the more expensive the chip</u>; Reducing the number of components will minimize cost but causes high power consumption, TRADEOFF!!!
- Cost

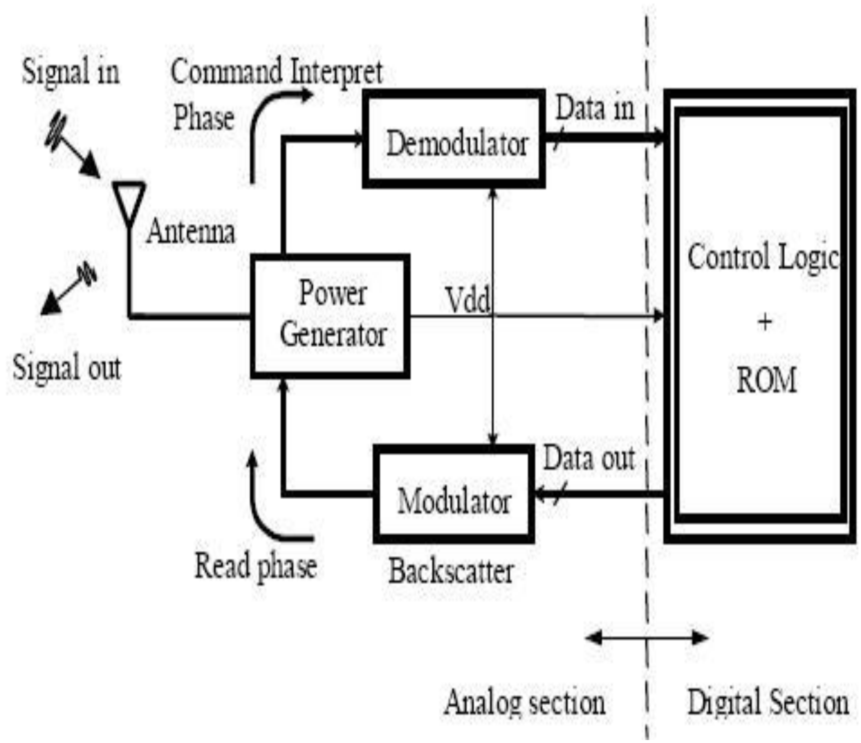
Physical implementation of Passive Tag

- A tag consists of an antenna attached to an electronic circuit
  - The antenna acts as a transducer between electromagnetic fields and electric energy .
- A transmission line transfer this energy to circuitry and vice versa
- The circuitry processes this energy, stores it, uses it and redirects it back through the transmission line and antenna



Physical implementation of Passive Tag

- The RF front end is responsible for bidirectional interfacing between the antenna and other functional blocks of the tag
- In the RF front end, energy and data are extracted from the input signal and sent to power supply, clock recovery and data processing circuitry
- Over voltage protection is located in the front end



What Passive Tags must do?

- Passive tags must <u>receive</u> and <u>rectify</u> the incoming signal for the <u>extraction of energy and information</u>
- It must <u>store and manage</u> the extracted energy to power the tag
- From the extracted information it <u>must establish a clocking signal</u> with which to drive its digital circuitry
- Through this circuitry, it must <u>process the information</u> and <u>make</u> the appropriate <u>modulations</u> of the incoming signal through backscatter modulation

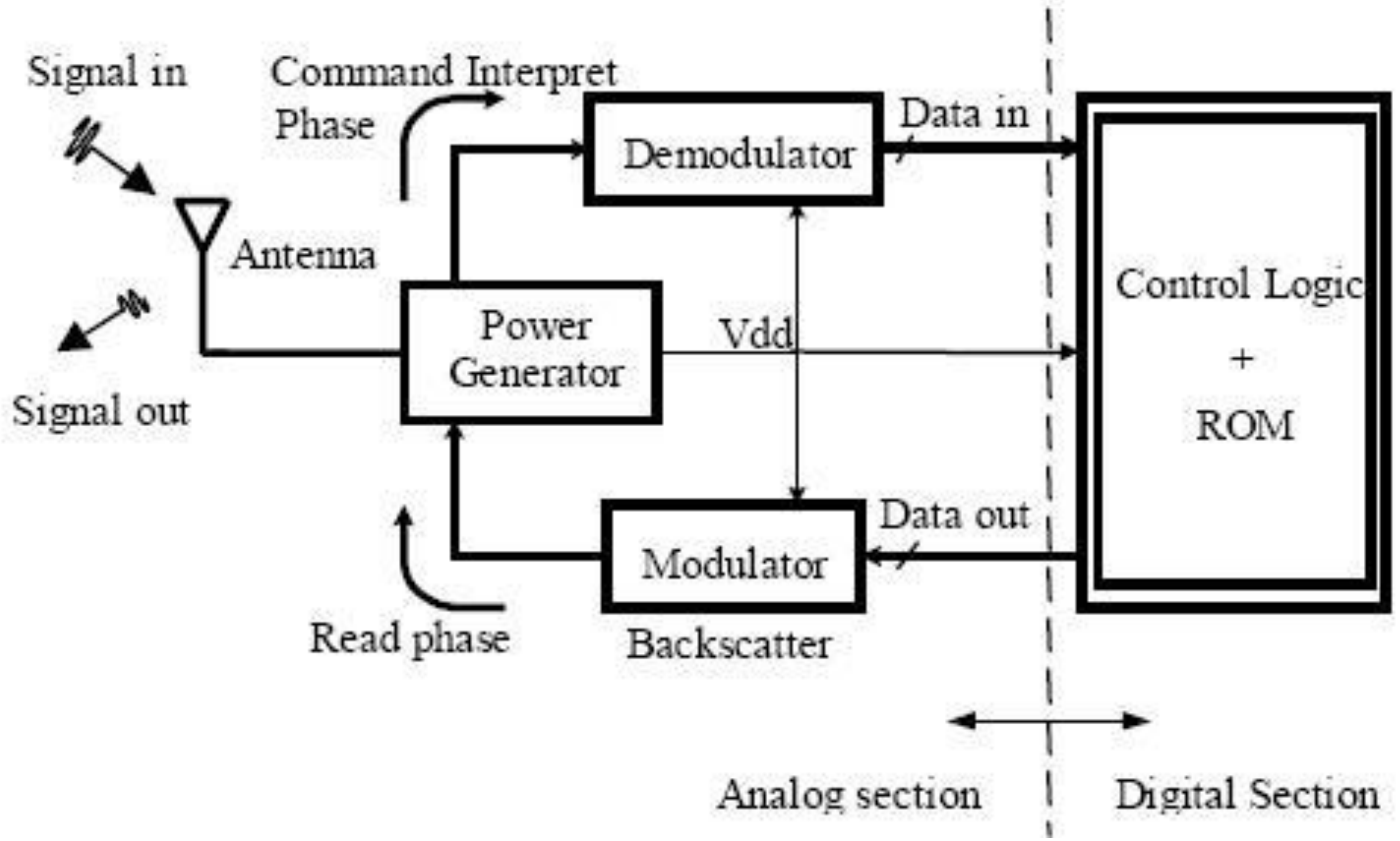
How communication with passive tag occurs?

- Data between reader and tag are transmitted in half-duplex mode.
- The reader continuously generates a RF carrier wave, which powers a passive tag when the tag is within its read range.
- The tag provides an acknowledgement to the reader by backscatter and the detected modulation of the field indicates the presence of the tag.
- The time taken for the tag to become fully functional is called the setup time. After this time, the reader requests for read/write access by sending appropriate instructions to the tag.

How communication with passive tags occurs?

- The demodulator recovers the input data stream and passes control logic circuitry deciphers the data to take corresponding action.
- After demodulation of the received instructions and handshaking, the information stored in the tag is transmitted back to the reader by backscattering.
- After all of the read/write operations are completed, the reader acknowledges the successful completion of the communication and the tag shuts off.

Architecture and Building Blocks of Passive Tags



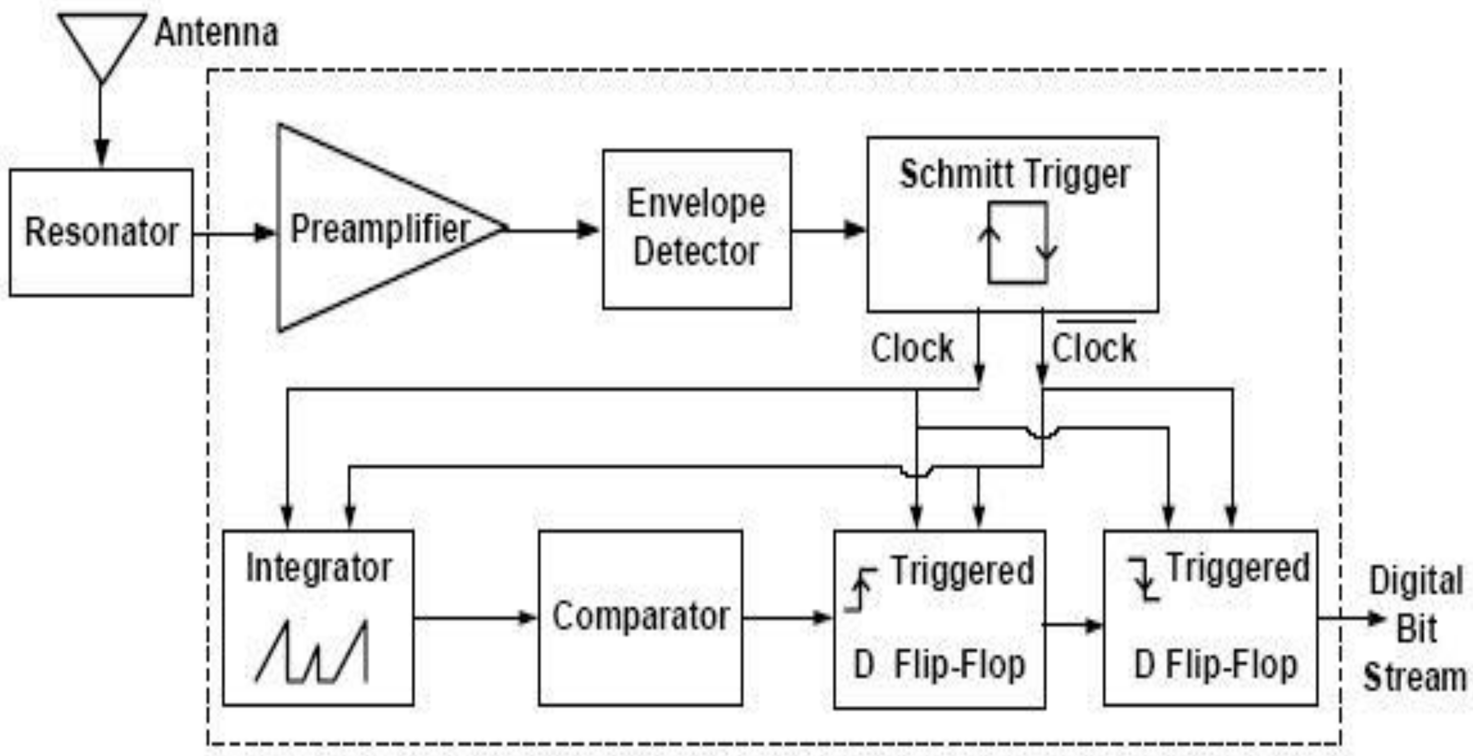
Antenna system

- Passive RFID tags are powered by the microwave signal received by the antenna
- The tag needs a minimum signal level at its antenna terminals to operate properly
- The tag will absorb some of the power to powering up itself and detecting information
- It will scatter some power to transmit information back to the reader

Data Demodulation

- In the case of passive operation, there is a strict power constraint on the tag's design
- BER might be sacrificed for the simplicity of design and power reduction in choosing the modulation scheme of the RFID system.
- In most of the passive RFID applications the data rate required is relatively low
- Bandwidth efficiency may be traded for simplicity in a passive RFID system
- Binary signaling should be preferred over M-ARY schemes.

Block Diagram of Demodulator



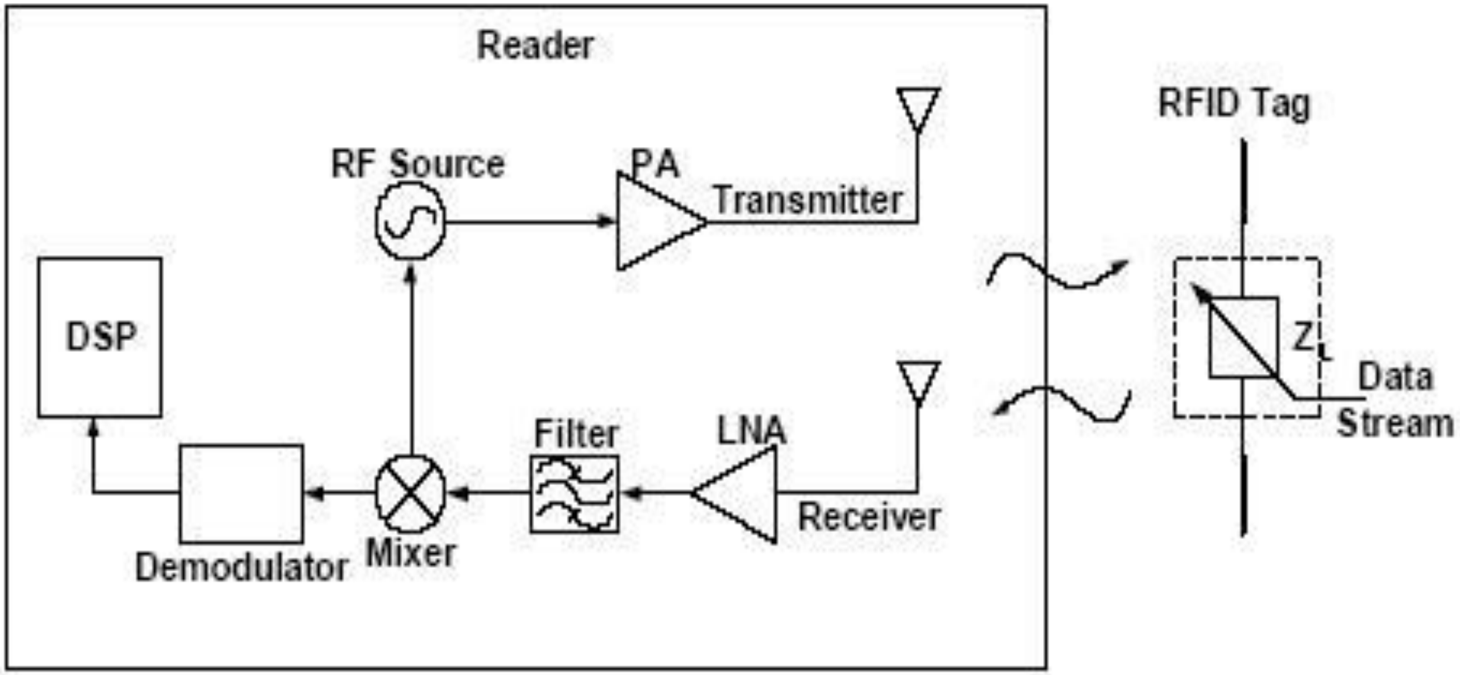
Description of Demodulator

- a preamplifier is used before the envelope detector to provide a DC level shift to the input signal and perform amplification for better detection.
- The envelope detector eliminates the carrier signal from the received signal and provides the baseband modulating signals
- Due to the non-idealities (i.e. ripples and peak clipping effects) at the output of the envelope detector, a Schmitt Trigger is used to recover the clear digital pulse train.
- The output of the Schmitt Trigger serves as the clock at the data rate for the rest of the processing circuitry
- The generated system clock is used to control the operation of the integrator and sample the output of comparator properly.

Backscatter modulation

- In the far-field, <u>variation of the tag's load impedance causes </u>an intended mismatch in impedance between the tag's antenna and load.
- This causes <u>some power to be reflected back </u>through the antenna and scattered, much like the antenna is radiating its own signal.
- The return scattered signal is detected and decoded by the reader.

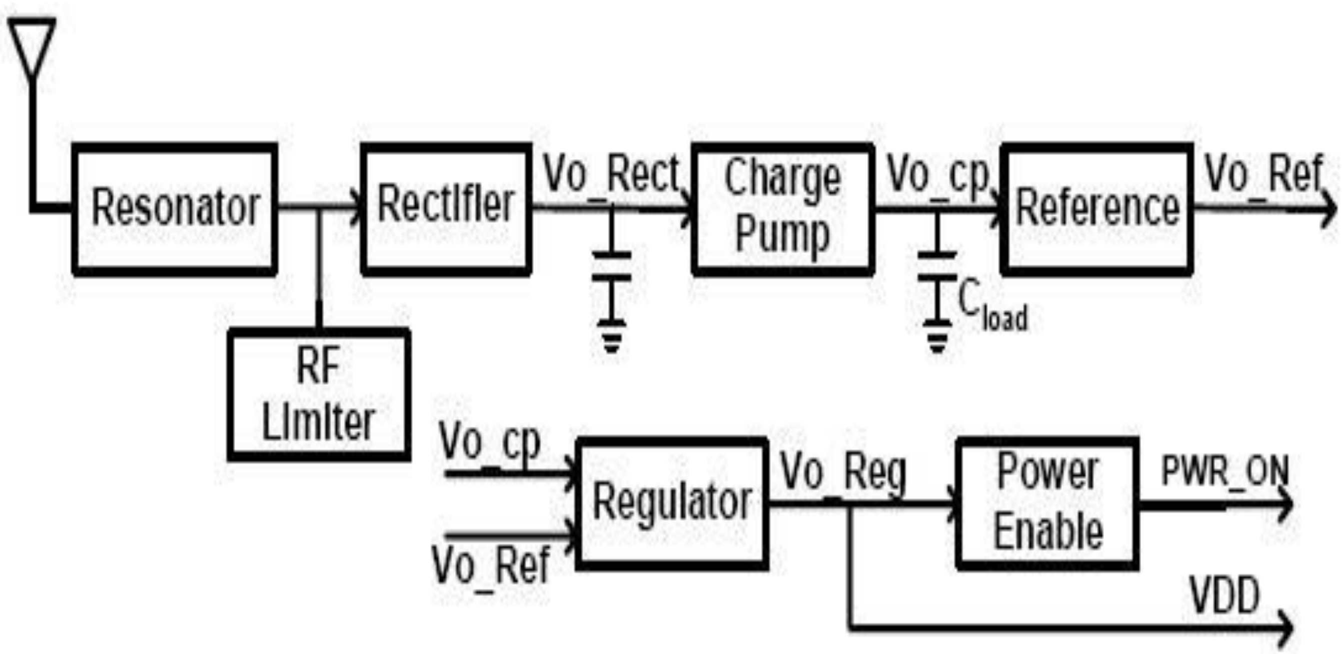
Backscatter communication



Power generation block

- The reader continuously generates a RF carrier wave, which powers a passive tag when the tag is within its read range.
- It makes use of RF-DC conversion and subsequent voltage regulation to obtain the desired stable power supply.
- An enable signal is used to indicate the successful generation of the power supply (VDD).
- A significant design challenge for the PG block is to maintain a stable supply voltage

Power generation block



Power generation block

- The resonator/matching network is connected between the antenna and the rectifier; and provides frequency selectivity and voltage gain to the system.
- The significant voltage gain enables the rectifier to overcome its dead zone limitations.
  - The intrinsic physical limitation on the operation of the devices (e.g. the cut-in voltage of the diodes) is called the dead zone of the device.
- The charge pump is used to boost the DC signal generated at the output of the rectifier
- The charge stored across the load capacitor of the charge pump (Cload) provides the unregulated supply voltage after the setup time.

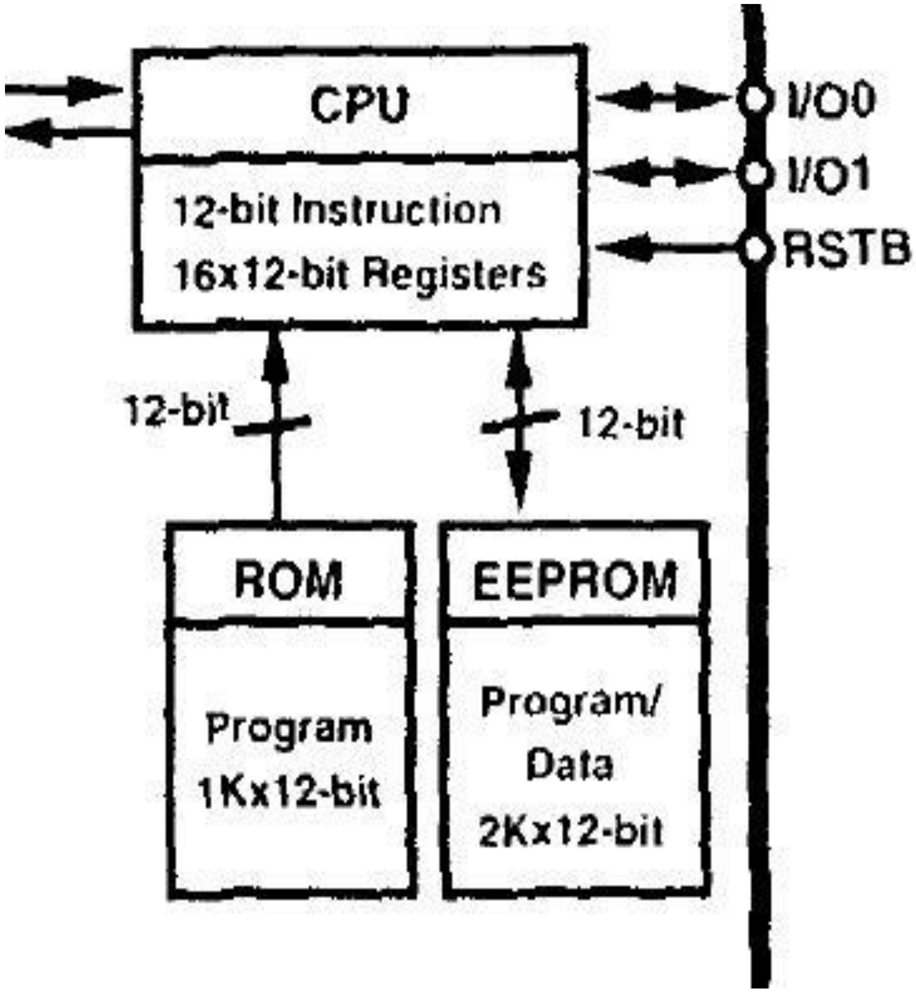
Power generation block

- The reference circuit aims at generation of an independent reference voltage to be used in voltage regulation

- The regulator is used to regulate the output of the charge pump and provide a stable power supply (VDD) to the rest of the chip. It minimizes the ripples and improves immunity to load variations

- The charge stored across the load capacitor of the charge pump (Cload) provides the unregulated supply voltage after the setup time.

Control Unit block



Control Unit block

- The instruction format is represented by 12b:
  - 4b opcode
  - 4b destination register address
  - 4b source register address

- The **instruction set has 29 operations** including an immediate addressing mode

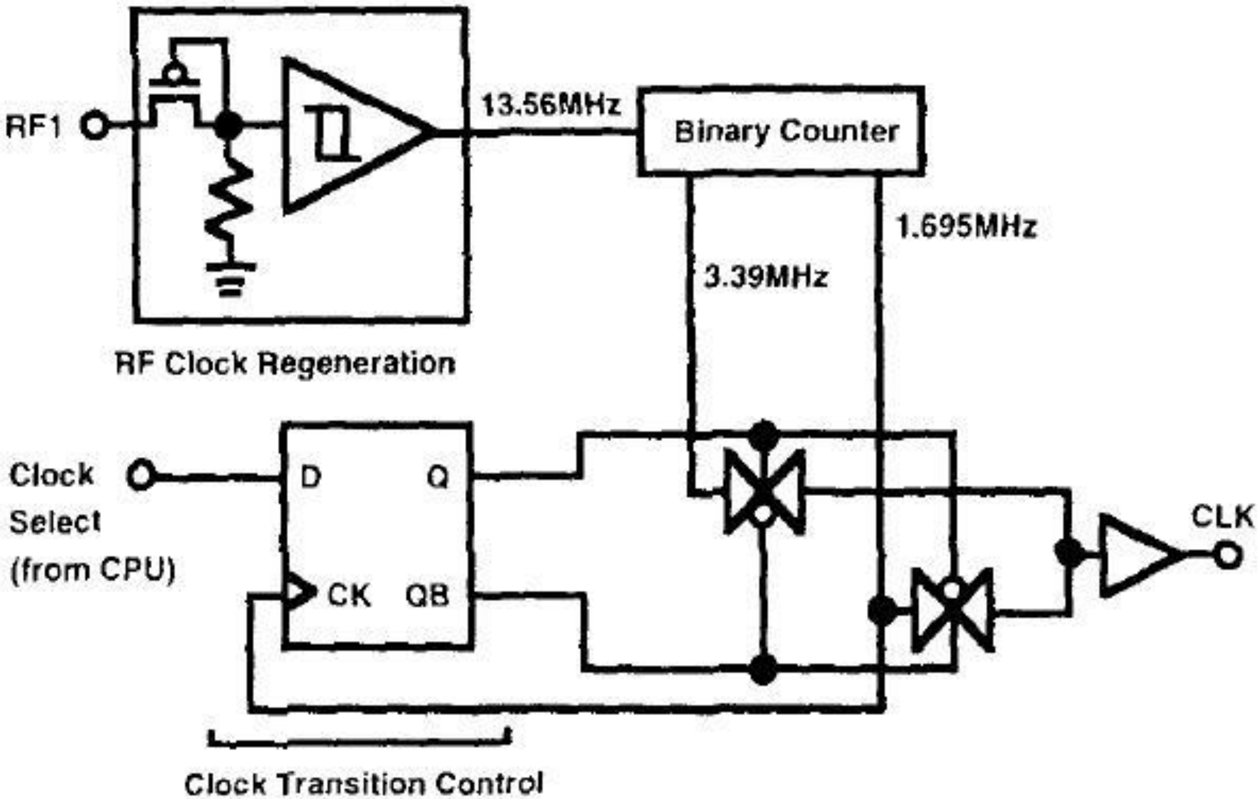
Control Unit block

- Registers in the CPU are organized as:
  - A Program counter
  - An Immediate register
  - An I/O register
  - 13 general purpose registers

- The demodulated data from RF block and modulation data from the CPU are transferred through the I/O register

- Data transfer between memory (ROM/EEPROM) and register is operated by LOAD/STORE instructions, in which the memory address field refers to a register

Clock Frequency Control Circuit



Clock Frequency Control Circuit

- The clocking signal is <u>used to drive the digital circuitry </u>of passive RFID tags

- In the data transmission, the lower frequency clock is selected since fewer CPU executions are required

Conclusion

- Passive RFID tags can work on different frequency bands, ranging from kHz to GHz.

- The choice of the frequency of operation affects the overall design of the tag, since it controls the complexity, the cost, and the range of operation

References

- http://www.hightechaid.com/tech/rfid/rfid_frequency.htm
- http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf
- Shariful Hasan Shaikot , RFID Passive Tag Architecture, Oklahoma State University
- http://www.gs1au.org/products/epcglobal/standards/


(TLG)Hades
NWS 2000/2
29/10/2000 02:21
nwsnet.de