Radio **F**requency **ID**entification (RFID)

Claudia Muñiz García

19 January 2007

RFID Tags and Readers

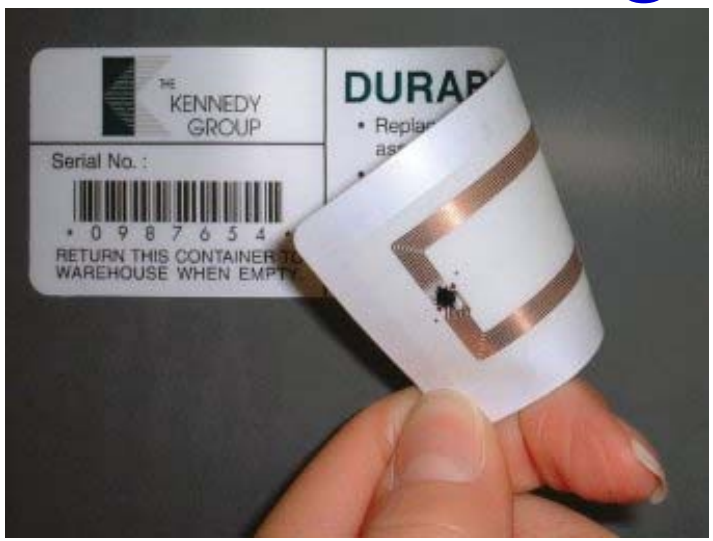
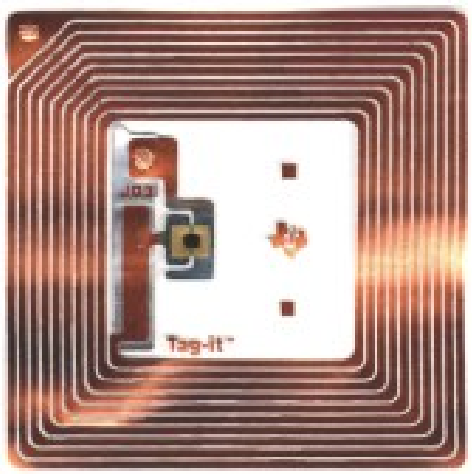


Photo: © Liz McIntyre 2006



RFID is useful when you need

- **No contact required → wireless**
- **Low cost**
  - Readers (R) and transponders (T)
  - Low power consumption (due to the operation in **near field** range)
  - No operating costs
- **Data** security
  - CRC for checking and even correcting transmissions
- **System** security
  - Cryptography to protect against eavesdropping/modification
- Moderate to high **data rates**
  - Animal ID → ≈6 Kbps (R→T) / 500 bps (T→ R)
  - Close Coupled Cards: ≥9.6 Kbps (symmetric)
  - Vicinity Coupled Cards: 1.65, 26.48 Kbps / 6.62, 26.48 Kbps
  - Proximity Coupled Cards: 106, 204, 408, 816 Kbaud
  - **G**lobal **TAG**s: 10, 40 Kbps (transponder)
- Flexibility
  - Reading and (re-)writing of transponders
  - Reusability
- Low failure rate
- Portability
- Low degradation and resistance against external conditions (weather, dirt)
- Independent of covering, direction, or position

RFID Applications & Markets

- Growing markets
  - 4,371,100,000 aircraft passengers last year, decrease processing time and increase security (assuming RFIDs are hard to fake)
- Some examples where RFID has improved function and/or reduced costs
  - **E**lectronic **A**rticle **S**urveillance (**anti-theft systems**; metallic tags which can be found in many shops – often behind the bar code)
  - **G**lobal **TAG** (Universal goods identification, supported by EAN.UCC)
  - Access Control
    - Passes (ID cards for employees), Passports, …
    - Hotel doors
  - Ticketing
    - Public Transport in combination with Secure Payment (**ICARE** & **CALYPSO**)
    - Ski turnstiles
  - Transport Systems (Signalling & Security in railways)
    - EURO-Cab , EURO-Radio, EURO-Loop, EURO-Balise
  - Animal ID (domestic animals, farm animals, carrier pigeon races, …)
  - Electronic vehicle immobilization (not only the locks, but also the engine)
  - Industrial Automation
    - Tool ID
    - Production Process - quality & progress control (i.e., automotive industry)
  - Medical Applications

Fundamental Operating Principles

Reader A read[/write] device which exchanges information with the

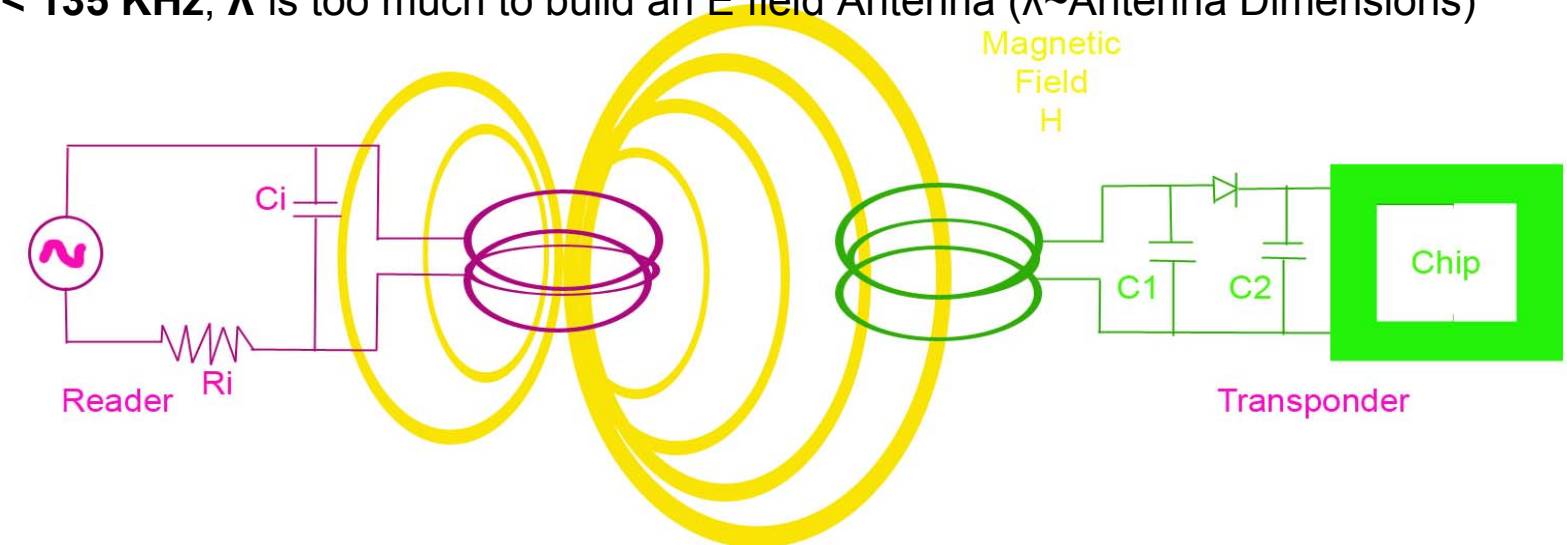
Transponder A device with (some) local storage:

- **Coupling element** (to obtain energy and data from reader's field)
- **Chip** (where data is stored[/processed])

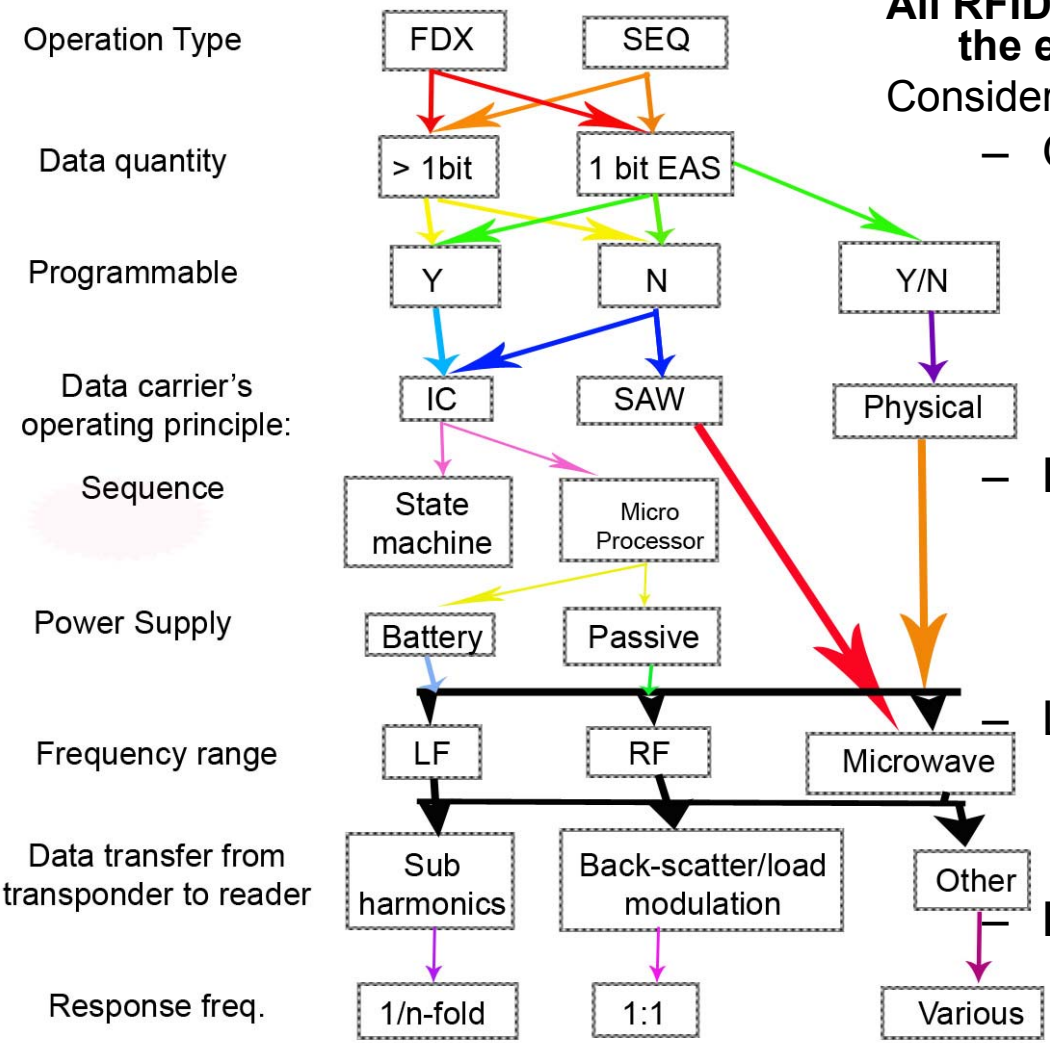
Interrogation zone Determined by the maximum distance between Rx & Tx, where the power provided by the transponder is enough for operation

Most RFID systems are **Inductively (Magnetic Field) coupled** and work within the **Near Field Zone (d<0.16λ, Power attenuation ~ R^{-6})** because:

- Power transmission is efficient, high power can be transmitted without causing interference with other devices due to the short range
- H field intensity can be increased with more windings in the coil or a ferrite
- **f < 135 KHz**, **λ** is too much to build an E field Antenna (λ~Antenna Dimensions)



Characteristics of RFID Systems



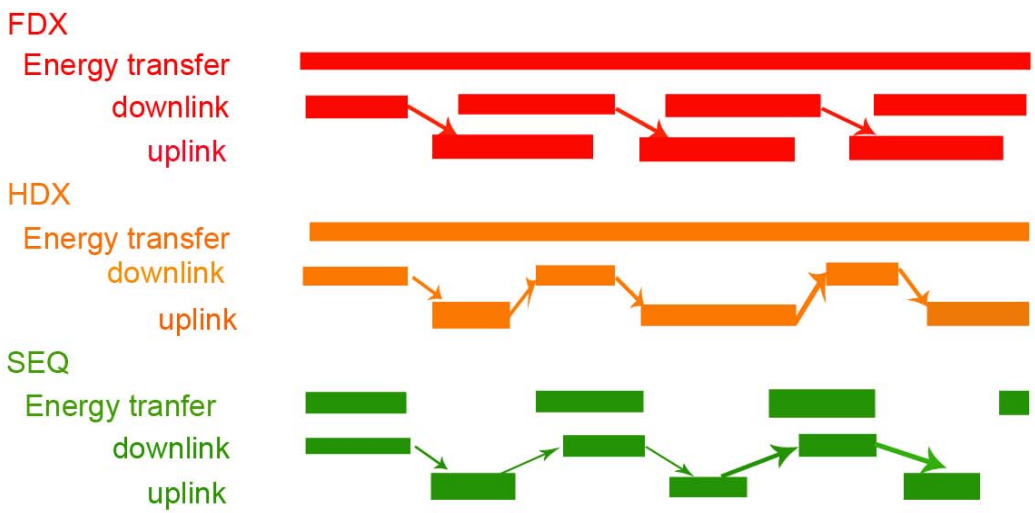
All RFID transponders are powered by rectifying the energy they get from the reader's field.

Consider **needs & choose** the suitable RFID solution

- Operating **Frequency**
  - Low Frequency → Inductive Coupling (Low power)
  - High Frequency → Electric Coupling (greater Range [2 to15m], Additional Battery needed - (The battery is only used to power the chip and retain stored data.))
- **Range** depends on
  - Speed & position of transponder in the **interrogation zone**.
  - Minimum distance among transponders.
- Level of **security**
  - Closed application (industry)
  - Public application (Currency, Goods) → ↑ requirements
- **Memory**
  - Capacity
  - (Re-)writability

Communication between Reader & Transponder

- **Reader:** Scans its **interrogation zone** by transmitting **f_R** continuously
- **Transponder:** When entering this zone a **sympathetic oscillation** occurs (**C1** is **resonant with the antenna (coil) at f_R), the coupled energy is employed to answer the reader either by:**
  - **Backscatter** (Reflection of the f_R creating an impedance dip @ Generator coil)
  - **Load Modulation (**Switching on and off a load resistor placed in the Transponder's Antenna will **change** its equivalent impedance **Z_T and vary the reflected voltage**)
  - **Load Modulation with Subcarrier** (Instead of using voltage variations to transmit information back to the reader what is done here is to create **2 sidebands at a subcarrier frequency** by combining f_R with a smaller frequency obtained by division: f_S)
  - **Subharmonics** (Use of a different frequency for the answer, obtained by division)
- Choices according to **power transmission from R→T** lead to 3 main systems: **FDX, HDX, SEQ.** Procedure:



Transponder

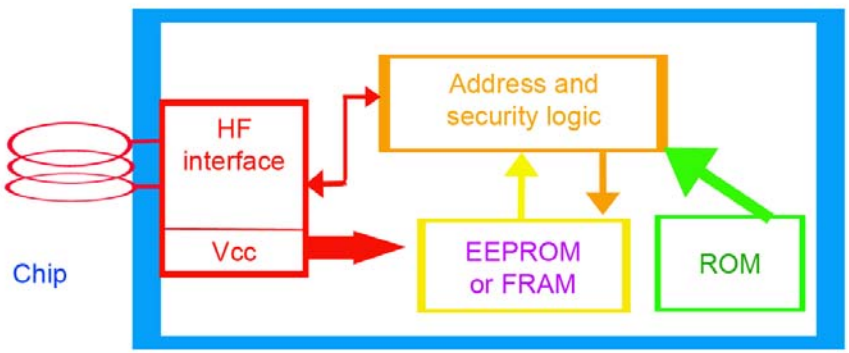
Complex transponders (those which are not **S**urface **A**coustic **W**ave or 1-bit) use **electronic circuits** to handle information, they form 2 main groups:

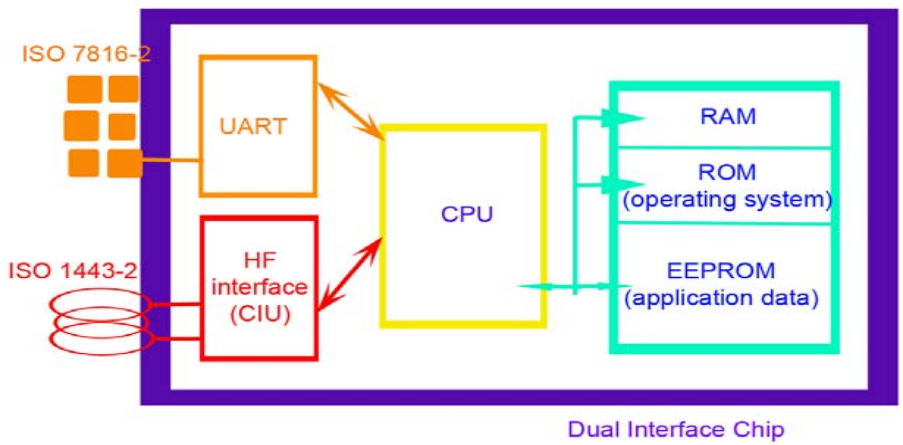
Transponders with Memory

- HF Interface
  - MoDem
  - Generation of system CLK by f_R division
  - Rectification to feed circuits with DC
- Memory - Read Only .. High End (Intelligent)
- **State Machine**
- Cryptographic Unit (optional)
  - to confirm that reader & transponder belong to the same system.

Transponders with Microprocessor

- More flexible than State Machines.
- Increasingly used in **Dual Interface Cards:**
  - **Contact** (↑ Security / Power)
    - Payment Applications, Mobile Phones (SIM)
  - **Contactless** (↓Power /Transaction Time)
    - Access Control
    - Ticketing (Small Payments)
- **P**ower **M**anagement **U**nit
  - power off inactive parts
- Evolution
  - Coprocessor (with DES)
  - Asymetric key algorithms (like RSA) → faster decryption



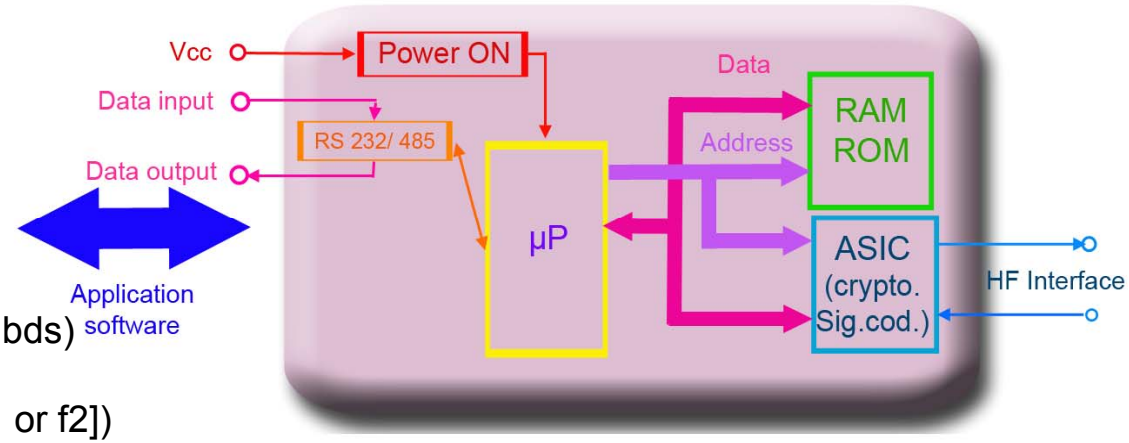


Reader: Control Unit

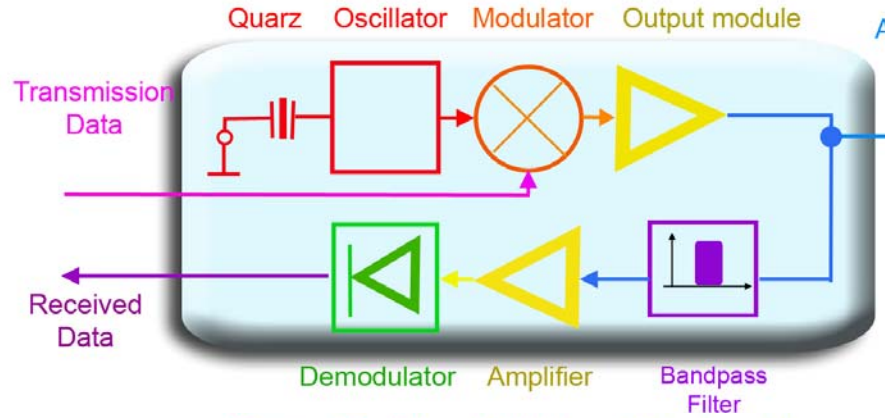
- **Control Unit**
  - Slave (of external appl.)
  - Master (of Transponder)
  - Signal Coding / Decoding
  - Data exchange:
    - With application Software

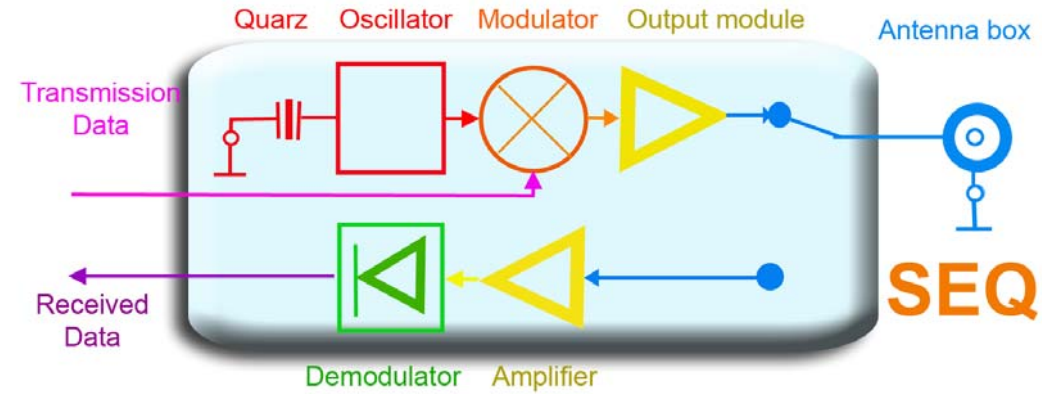
    (via RS232/485, NRZ @ 1200 bds)
    - With HF interface

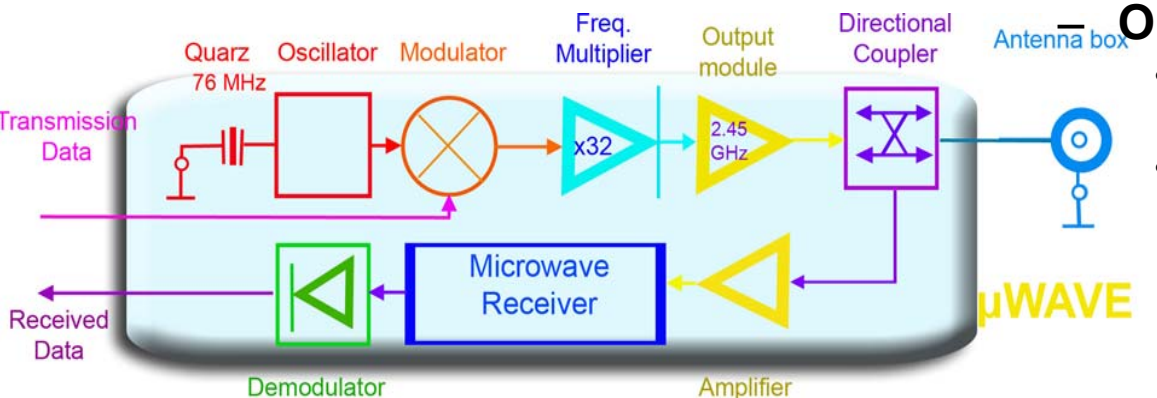
    (via ASK [HF on/off] or FSK [f1 or f2])
  - Anticollision Algorithms: To allow many transponders inside the same interrogation zone
  - Encryption / Decryption of Data: To increase security of transmission
  - Authentication Procedures: To recognize application's transponders among all
- **HF Interface**
  - Generation of power to activate & supply the transponder
  - Different configurations depending upon
    - Coupling (Magnetic or Electric field)
    - Communication Sequence (HDX, FDX or SEQ)
  - MoDem (2 isolated signal paths):
    - Transmitter
    - Receiver



Reader's HF Interface







- Since there is a resonator at the antenna, tradeoff with **Q factor** must be taken into account:
  - ↑Q → ↑ Power efficiency & ↓ Band
  - ↓Band → ↓ Data Rate because B·T=1 (in 4 ASK)
- Different designs for different requirements
  - **Portable**
    - Animal ID, Payments, Public Transport…
    - Independent (LCD display + Keyboard or RS232)
  - **Industry**
    - Standardized bus interface
    - Low cost with mass production (i.e. cars)
  - **OEM Readers**
    - Customer systems (Access control, Till, Robots, …)
    - Packaged or unpackaged

Main Frequency Bands

RFID systems generate & radiate EM waves so, in order to avoid interference with another radio systems, they operate at very **short distances** within the **I**ndustrial **S**cientific **M**edical **frequency range**{*Regulated by ISO 18000}**:**

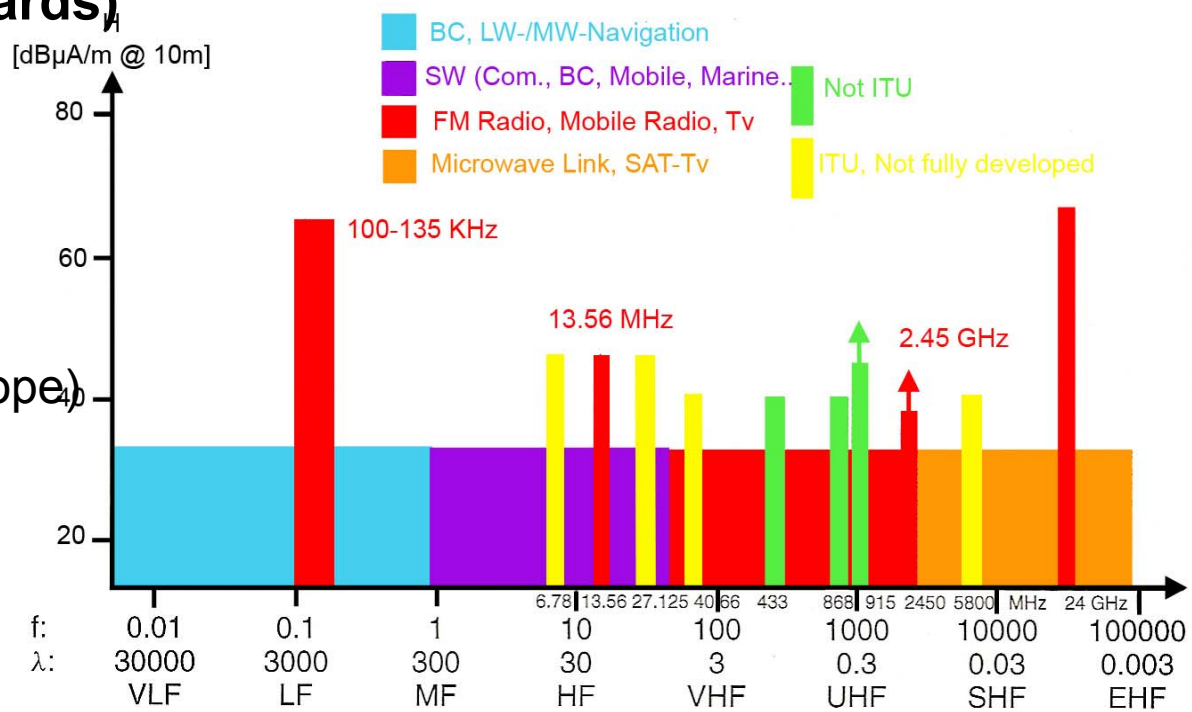
- 0-135 KHz* **(ISO 11785, Animal ID)**
- 6.78 MHz (not yet in Germany)
- **13.56 MHz (ISO 14443 Proximity Coupled Cards, 15693 Vicinity Coupled Cards)***
- 27.125 MHz
- 40.68 MHz
- 433.92 MHz
- 869.0 MHz

(ISO 10374, GTAG)

- 915.0 MHz (not in Europe)
- 2.45 GHz*/ 5.8 GHz*

(Remote Coupling)

- 24.125 GHz



Data Integrity

Recognize errors & perform corrective action

- Parity Checking
- Longitudinal Redundancy Check
- **C**yclic **R**edundancy **C**heck (CRC)
  - Mostly Used, **better** because an **even** number of **errors** is **also detected.**
  - Uses a polynomial to detect many errors

Data Integrity

Anticollision

- RFID is characterised by:
  - **Burst** (Brief periods of high activity, between pauses of different durations)
  - Data flow only R←→T (not between Transponders)
  - **Shared channel**.
  - These lead to **collisions**.
- **S**pace **D**ivision **M**ultiple **A**ccess
  - Array Antennas(~λ)
  - Expensive & Only feasible @ f>850 MHz
- **F**requency **D**omain **M**ultiple **A**ccess
  - 1 synchronizing frequency, N subcarriers (one uplink/transponder)
  - Very expensive reader
- **T**ime **D**omain **M**ultiple **A**ccess
  - Different timeslots, one for each.
- **ALOHA**
  - Normal ($S_{MÁX}$ = 18.4% with 50% load)
  - Slotted Aloha (double $S_{MÁX}$ = 36.8% with 100% load)
  - Dynamic S.A. (better eficiency, variable number of slots)
- **Binary Search**
  - With Manchester Coding, the precise position of the bit with collision can be detected to select a desired transponder among all of them.

Data Security

- Cryptographic processing & authentication are **expensive** (both Silicon and power → use **only when needed**
- When used in **ticketing & payment** applications, data transfer must be secure - against:
  - Unauthorized reading of data to modify / duplicate it
  - Placing of foreign data carriers to access services / buildings without payment / authorization
  - Eavesdropping to replay data & fraud

Data Security Procedures

- **Mutual Symmetrical Authentication [ISO 9798-2]**
  - Both participants check each other
    - **Keys not transmitted, only random numbers** → avoids replay attack
    - All use the same key (potential danger)
- Authentication by means of **Derived Keys**
    - **Each transponder has its own key**, which is checked at the Security Authentication Module at the reader with a master key.
- **Encrypted Data** Transfer
  - Attacks (Passive - only eavesdropping vs. Active)
  - Transmission
    - **Symmetric** cipher (both must know the key)
    - **Asymmetric** cipher (key is not needed to decipher)
    - **Block** cipher (more calculations required)
    - **Sequential** cipher (simple & cheap)
    - **Stream** cipher
      - Vernam Cipher (One key each time)
      - Pseudorandom Sequence (Use of LFSR)

Questions & Answers

Thank you!!!