ECE 5990

Note 4

NFC RFID Systems

Edwin C. Kan
School of Electrical and Computer Engineering
Cornell University
Fall 2014

Outline

- Auto-ID system comparison
- Packaging and types of near-range reading
- The 1-bit transponder
- NFC RFID circuits

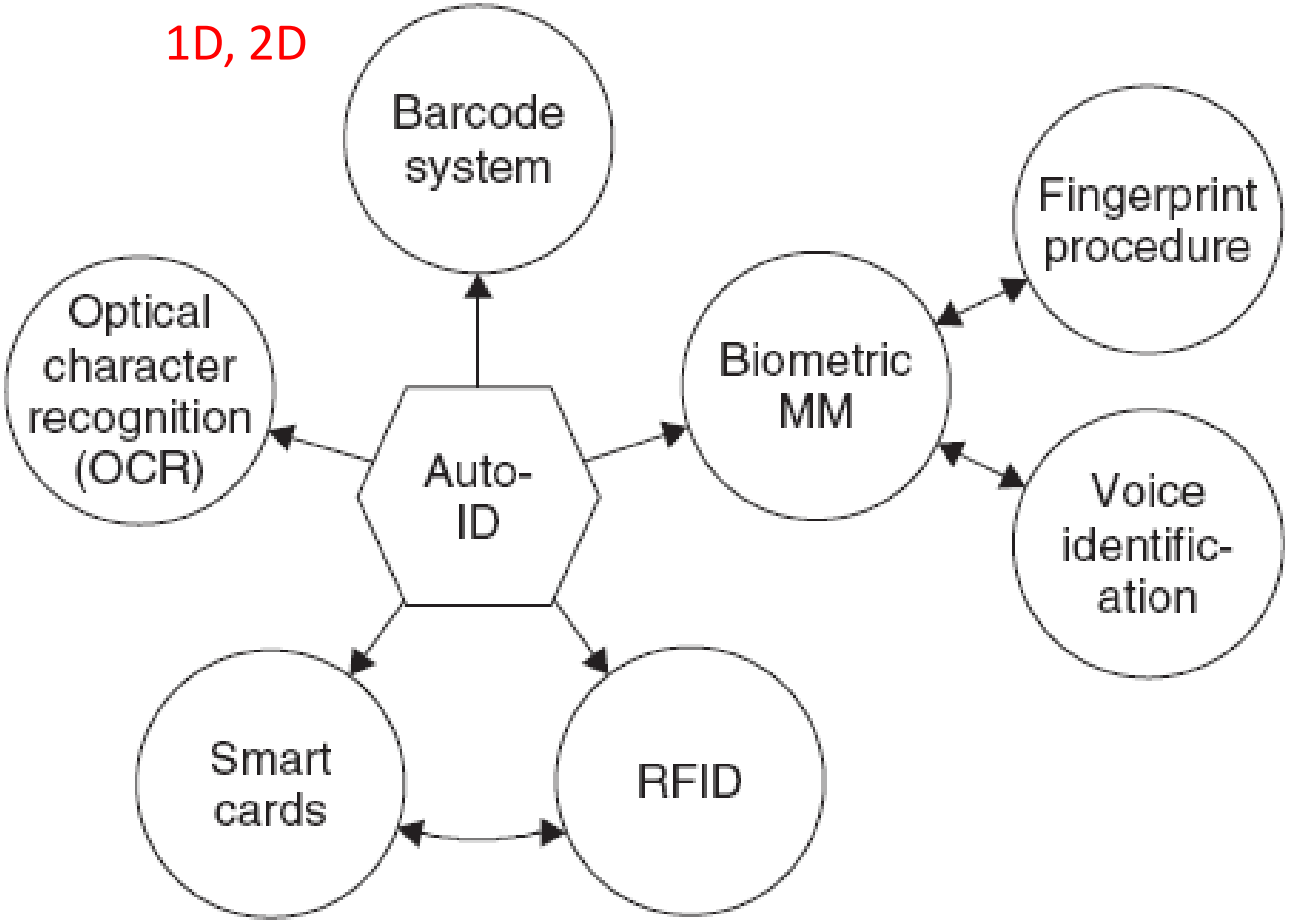
Quotable Quotes

"**The Galvanic Circuit Investigated Mathematically**" stated Ohm's law for electromotive force acting between the extremities of any part of a circuit is the product of the strength of the current, and the resistance of that part of the circuit."

— Georg S. Ohm (1789 – 1854)

Auto-ID System Comparison
(Most of the Time the ID is Read One by One)

1D, 2D



Electrical contact
Magnetic strip

NFC
Electromagnetic Type (NF)

Optical Bar Codes

- Bars and gaps designed for digital ID
- Alignment marks to counter optical distortion
- One-way reading; cheap; counterfeit concerns
- EAN (European Article Number) and UPC (Universal Product Code) in US; UPC is a subset of EAN.

European Article Number (EAN)

Country		Company Identifier					Manufacturer's Item Number					CD
4	0	1	2	3	4	5	0	8	1	5	0	9
FRG		Company Name					Chocolate Rabbit 100g					

- 13 digits: country (2); company (5); item ID (5); check digit (1)
- Other popular codes: codabar (medical); 2/5 (auto industry); 39 (libraries)

Biometric Procedures

- Fingerprints (dactyloscopy)
- Keypad with signature
- Retina scan
- Voice identification: Edna Mode in “The Incredibles”: http://www.youtube.com/watch?v=98J425wZvE0

False Positive and Negative in ID

- False positive: an attacker mistaken as THE legal owner of ID
- False negative: THE legal owner of ID cannot be identified
- Statistics for false positive and negative have to be established by **experimental testing** of a large representative population.
- The same principle of testing statistics applies to disease identification (diagnostics), pharmacy, cyber security, wireless communication, etc.

Error Tolerance and Multiple ID

When ID reading error is more tolerated (or equivalently the ID is going through an error-correction code that corrects more bits in error):

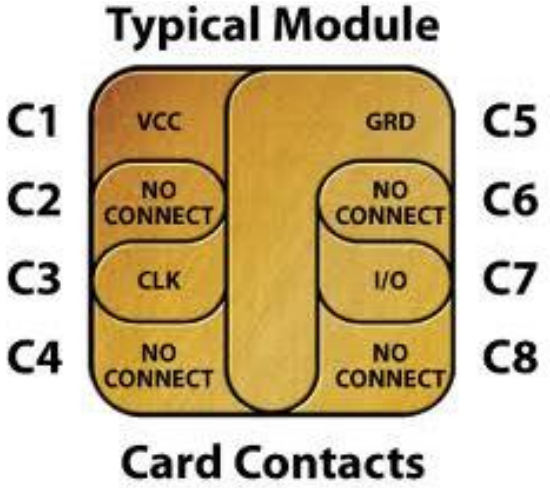
- False negative is lower (the true user will not be denied)
- False positive probability is higher (the attacker needs less efforts)

Multiple ID is used before authentication

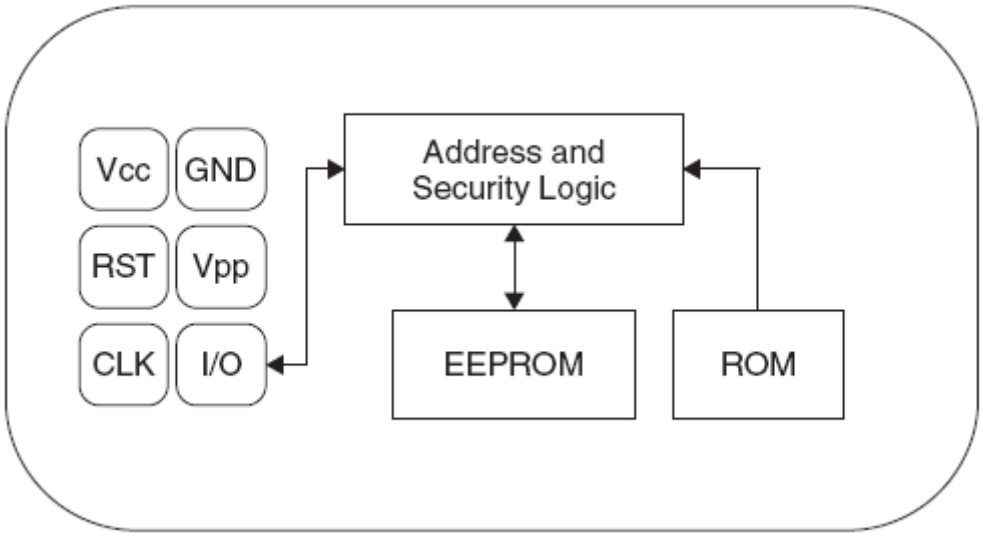
- False negative is higher (the legal user needs more effort or time to get authentication)
- Harder for attackers to get simultaneous authentic ID

Smart Cards

- Magnetic strip or 2D bar code (only one way identifying)
- Galvanic contacts (two-way duplex)
- RF link (NFC RFID)

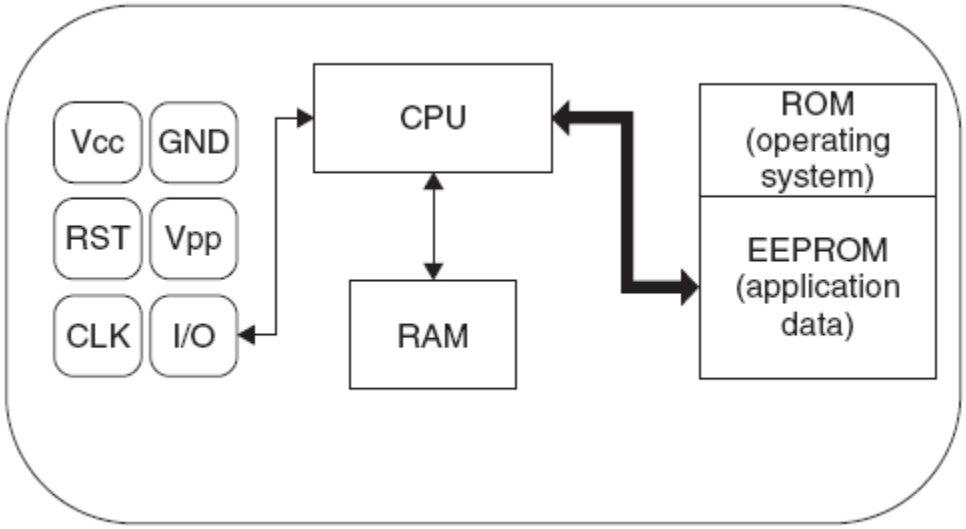


Contact Based Smart Cards

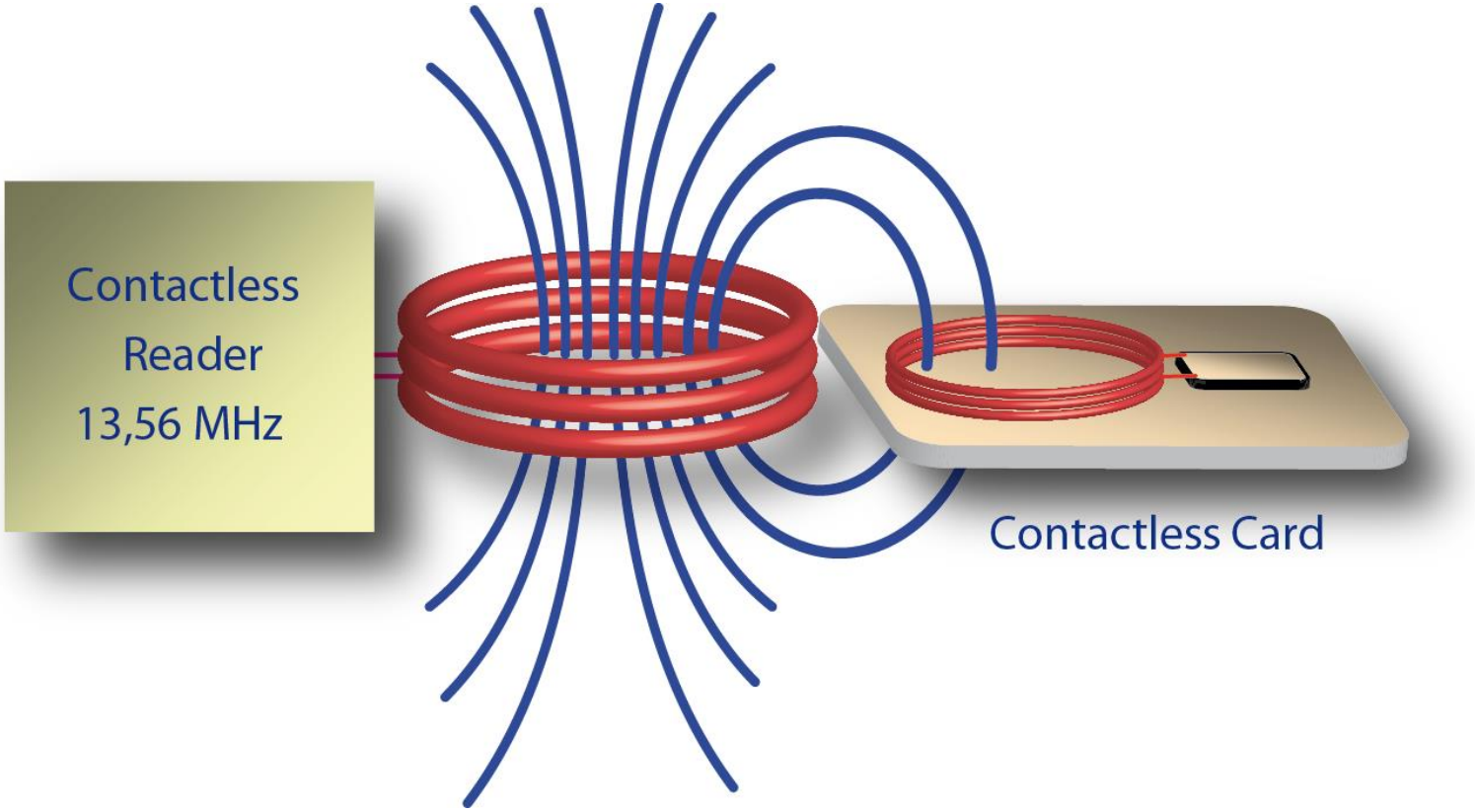


"Memory Card"

"Processor Card"



Contactless Smart Cards



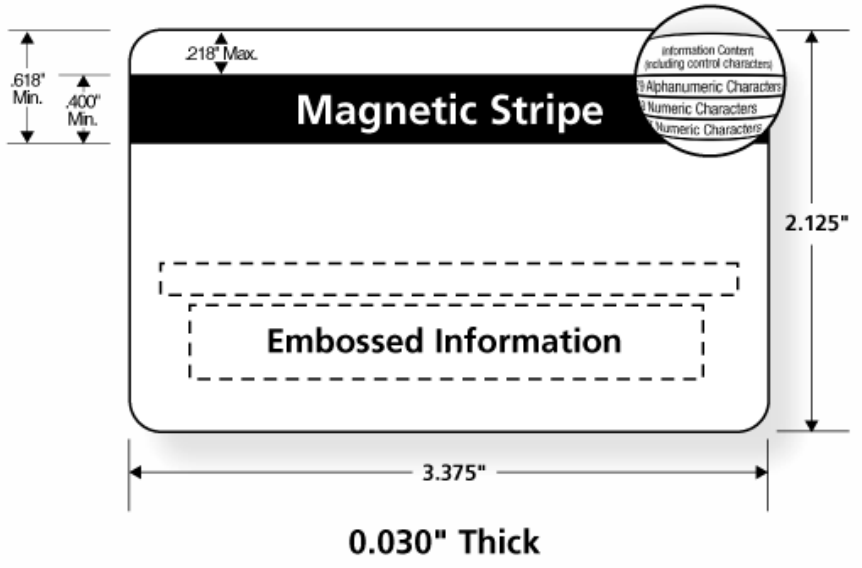
More later…

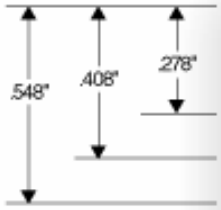
ID Tool Comparison

System Parameter	Barcode	OCR	Voice recognition	Biometry	Contact smart card	NFC RFID
Data quantity (bytes)	1 – 100	1 – 100	–	–	12 – 64K	12 – 64K
Data density	Low	Low	High	High	Very high	Very high
Reader price	Very low	Low	High	Very high	Low	Very low
Readability to people	Some	Easy	Easy	Difficult	Impossible	Impossible
Dirt/damp	Bad	Bad	–	Bad	Possible	No
Card cost	< 0.1¢	< 0.1¢	–	–	~ $1	~ $0.2
Reader cost	~ $50	~ $50	~ $1,000	~$2,000	~ $200	Cell phone or ~$50
Reading speed	~ 3s	~ 3s	> 5 s	> 10 s	~ 3 s	< 0.5 s
Major concerns	Covering, copying	Counter-feiting	Noise, reliability	Expense, false neg.	Contact wear	Eavesdrop-ping

Symbols for ID

- Visual/scanning codes:
- Magnetic reading:



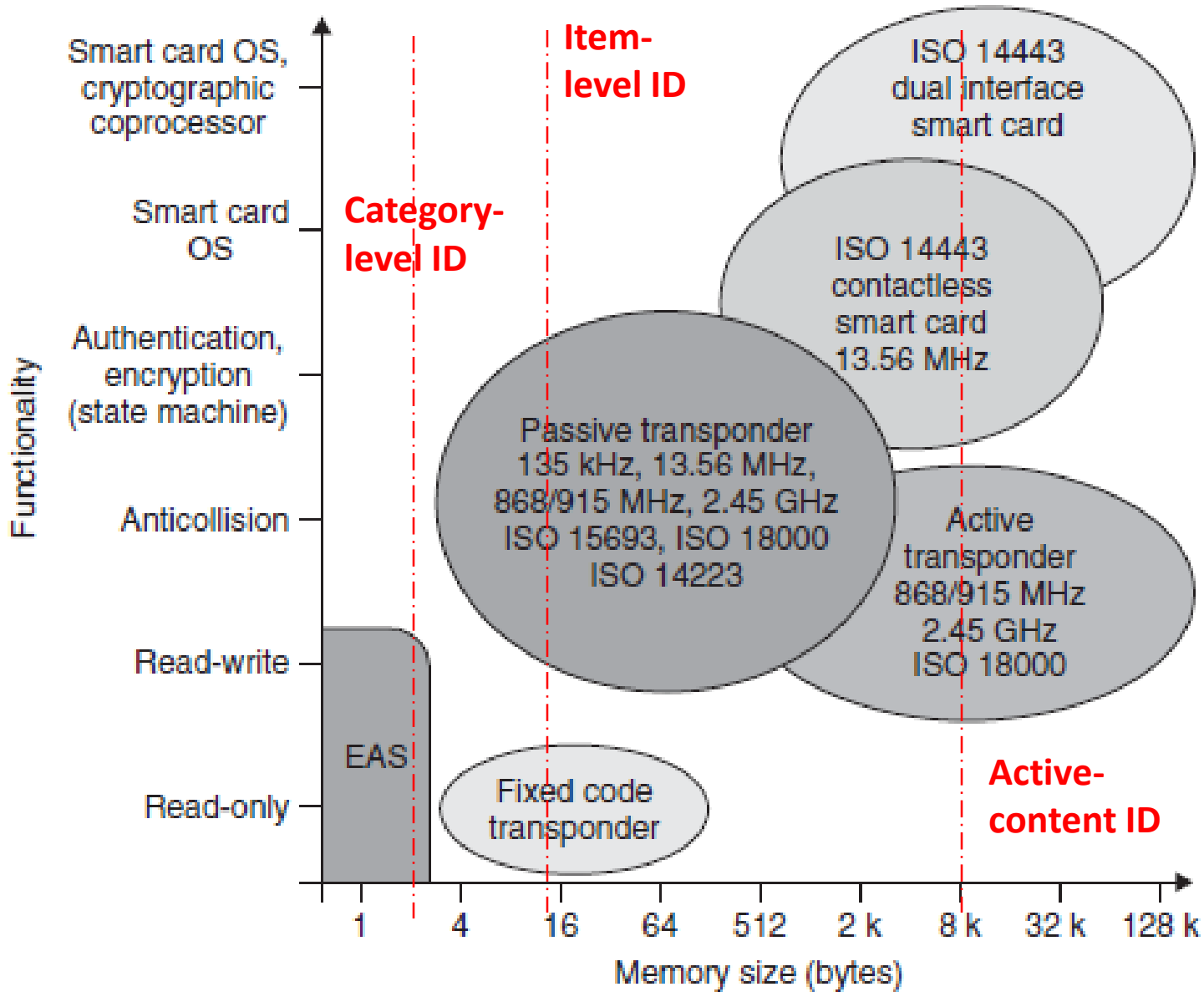


0.233"			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

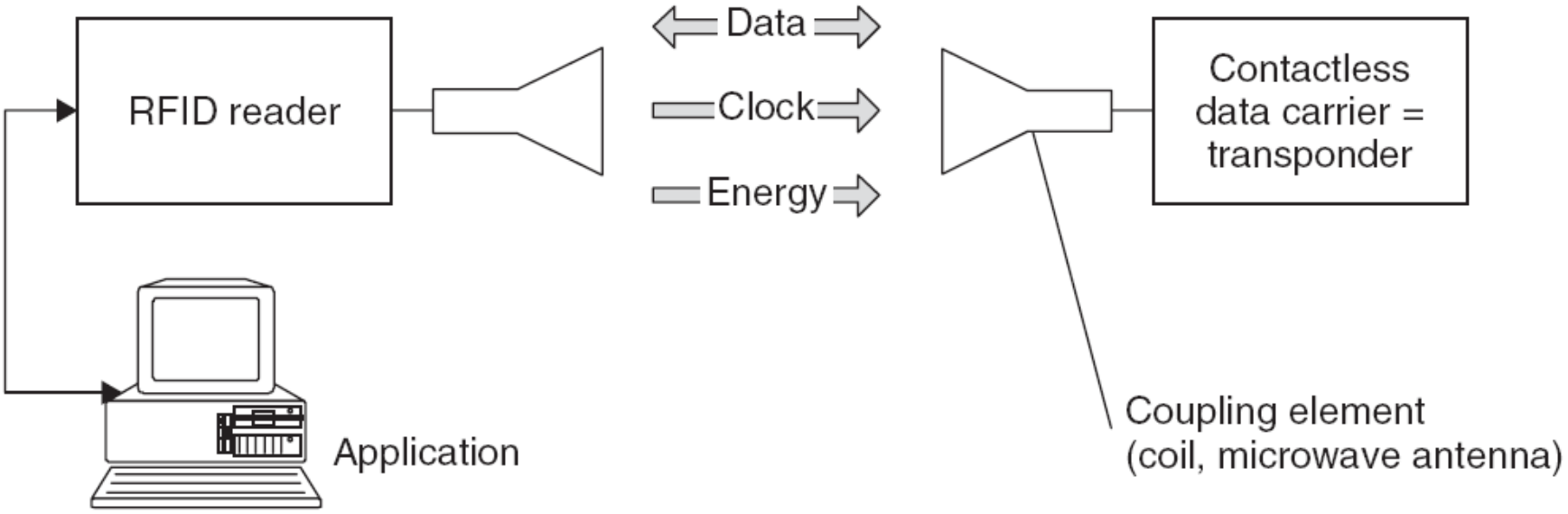
Symbols for RFID

VS.

RFID Cards: Functions and Capacity



Contactless RFID NFC Card



- Contactless reading gives high reliability and read speed
- More vulnerable to eavesdropping than Galvanic contacts
- Presently the NFC standard has been adopted by Android OS. For example, a Google Moto phone call read/write NFC tags with a download Applet.

Outline

- Auto-ID system comparison
- Packaging and types of near-range reading
- The 1-bit transponder
- NFC RFID circuits

Types of NFC

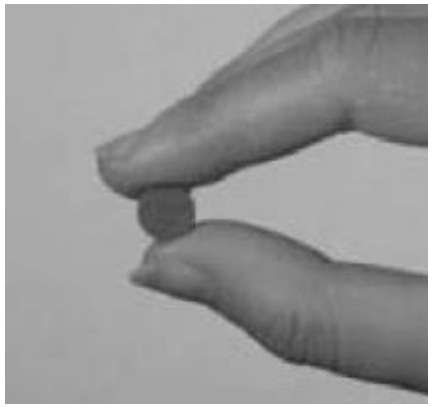
1-bit transponder as in electronic article surveillance (EAS)

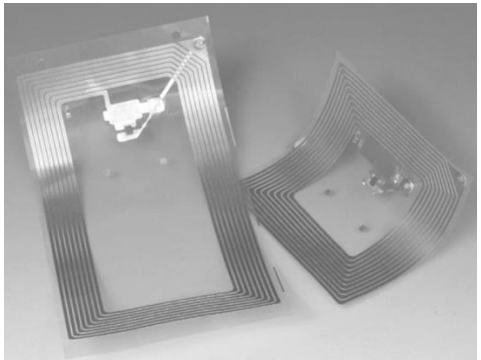
Interrupted near-field magnetic or electromagnetic coupling

96 – 16K bit stored in:

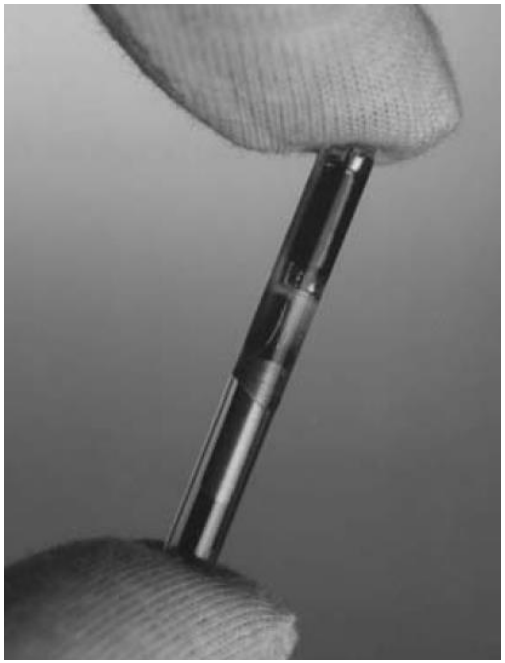
- EEPROM (embedded, most popular)
- FeRAM (lower power, but expensive)
- ROM (not field writable)
- One-time PROM
- SRAM (need an enclosed battery)

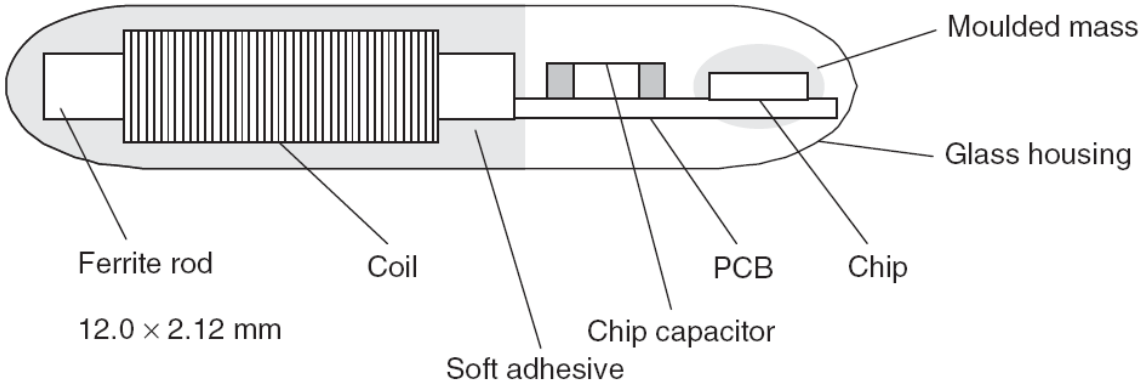
Packaging of NFC: 2D Disks/Cards



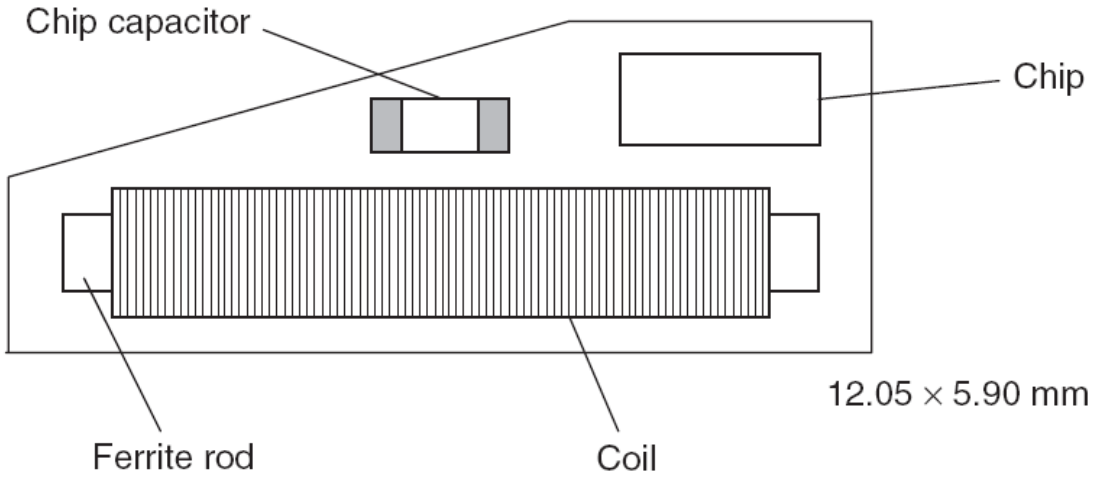


Packaging of NFC: 3D Tubes

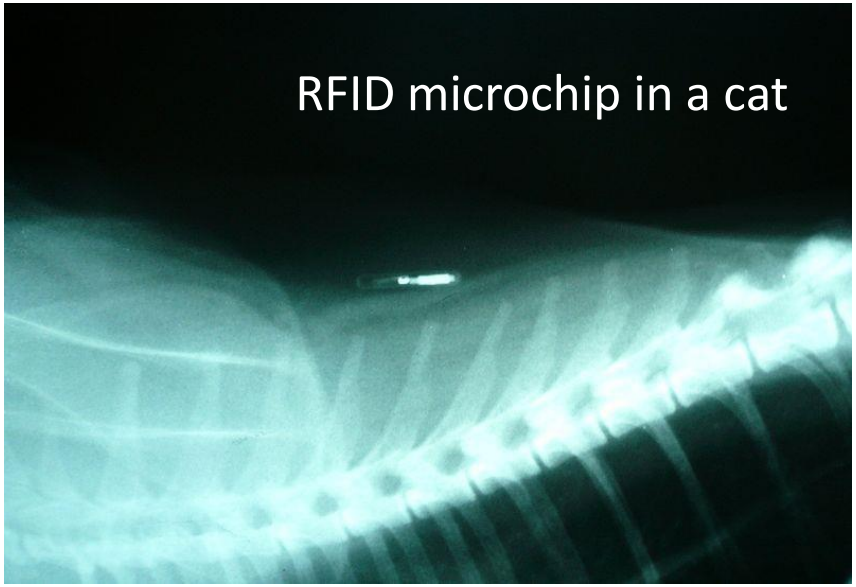




Mostly used in pet ID



Pet Microchipping



NFC Frequencies and Loads

- Low frequency (LF, 125 – 134 kHz): 100 – 300 kHz.
- High frequency (HF, 13.56MHz) or radio frequency (RF, VHF): 30 – 300 MHz
- Interactive spectrum map available at: fcc.gov
- Load modulation (most popular for NFC): Inductive and capacitive load coupling
- Sub-harmonic modulation: carrier and base bands
- Harmonic modulation: 2^{nd} and 3^{rd} harmonics, often with sub-harmonic modulation as well.

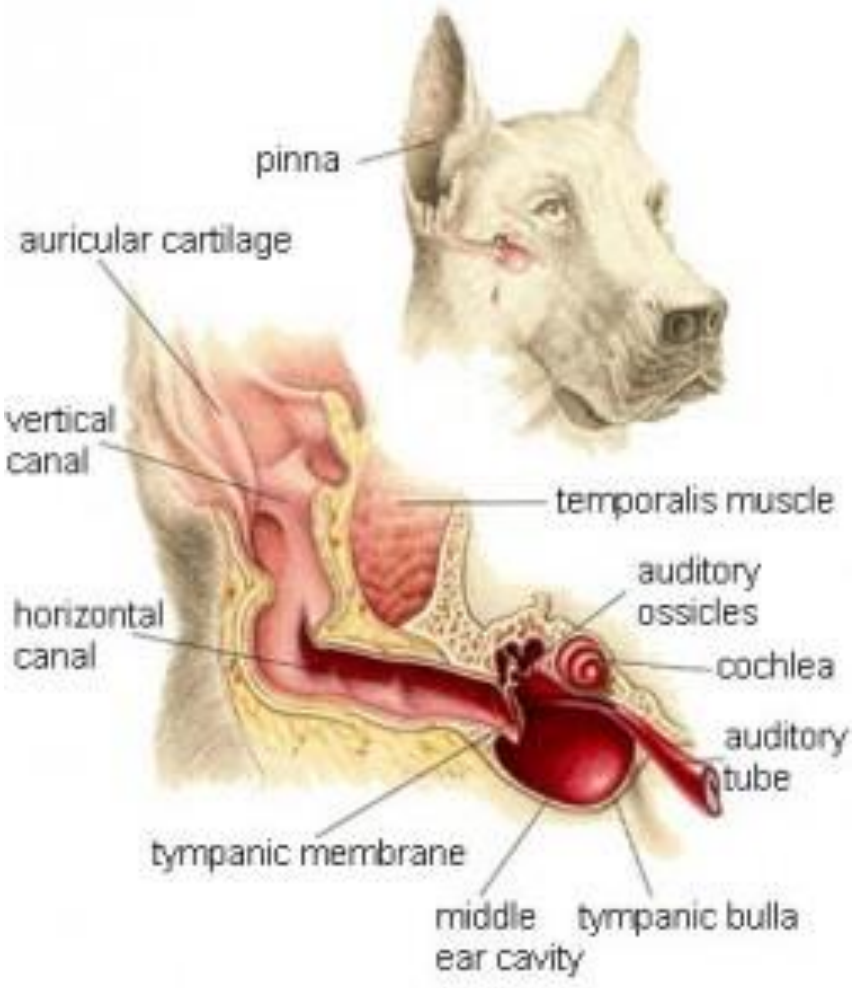
Animal Tracking by NFC RFID

- Domestic animal tracking: disease control, lost-and-found, etc.
- Wildlife tracking: disease control, population, environment
- Night and day: comparison with a tag based on imaging

The Roaming Dog Project

- Remote tracking of dog vaccination by RFID tagging of dog ears

ACC&D
Alliance for Contraception in CATS & DOGS



Outline

- Auto-ID system comparison
- Packaging and types of near-range reading
- The 1-bit transponder
- NFC RFID circuits

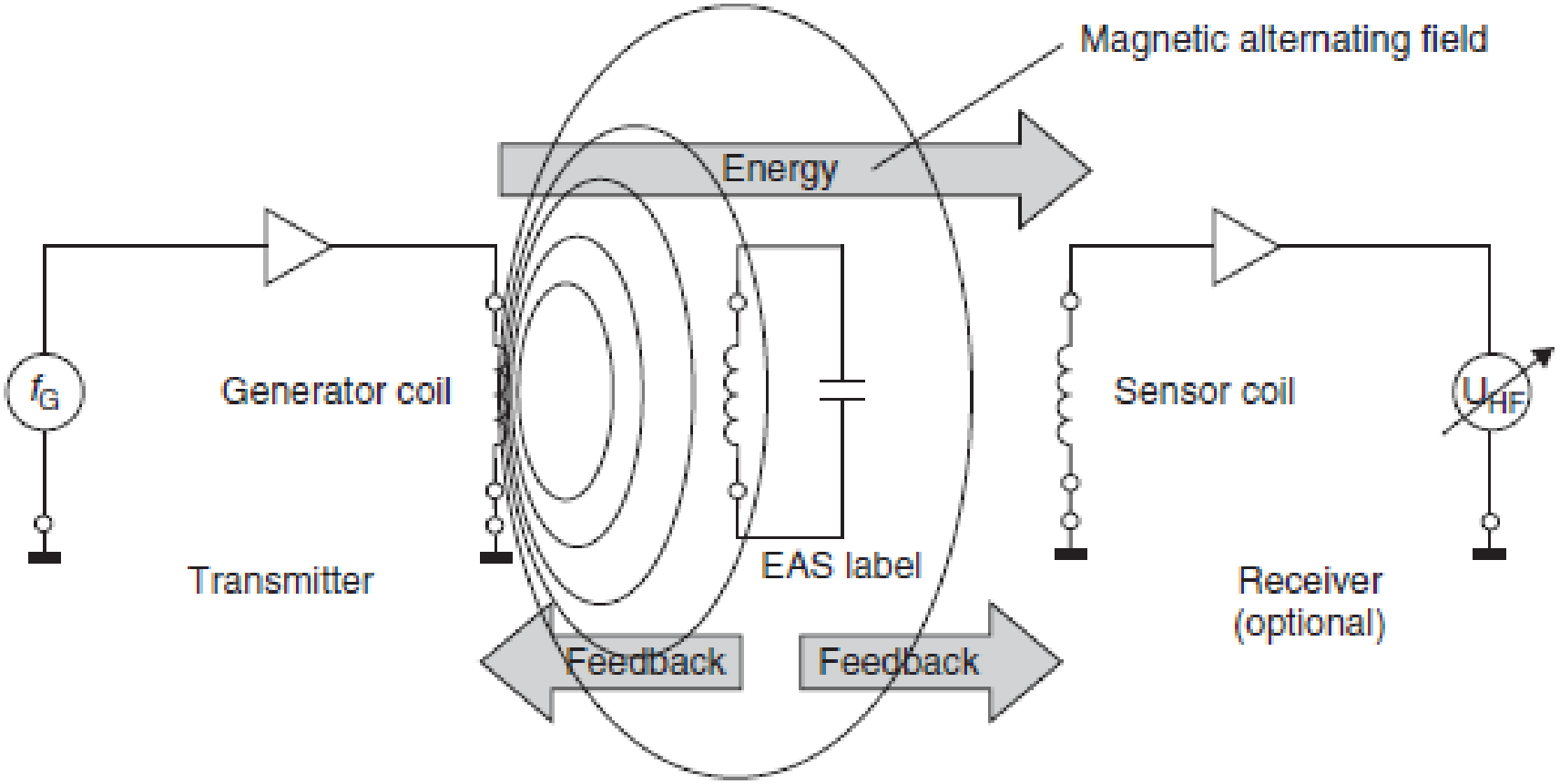
1-Bit Transponders (EAS)

EAS: electronic article surveillance

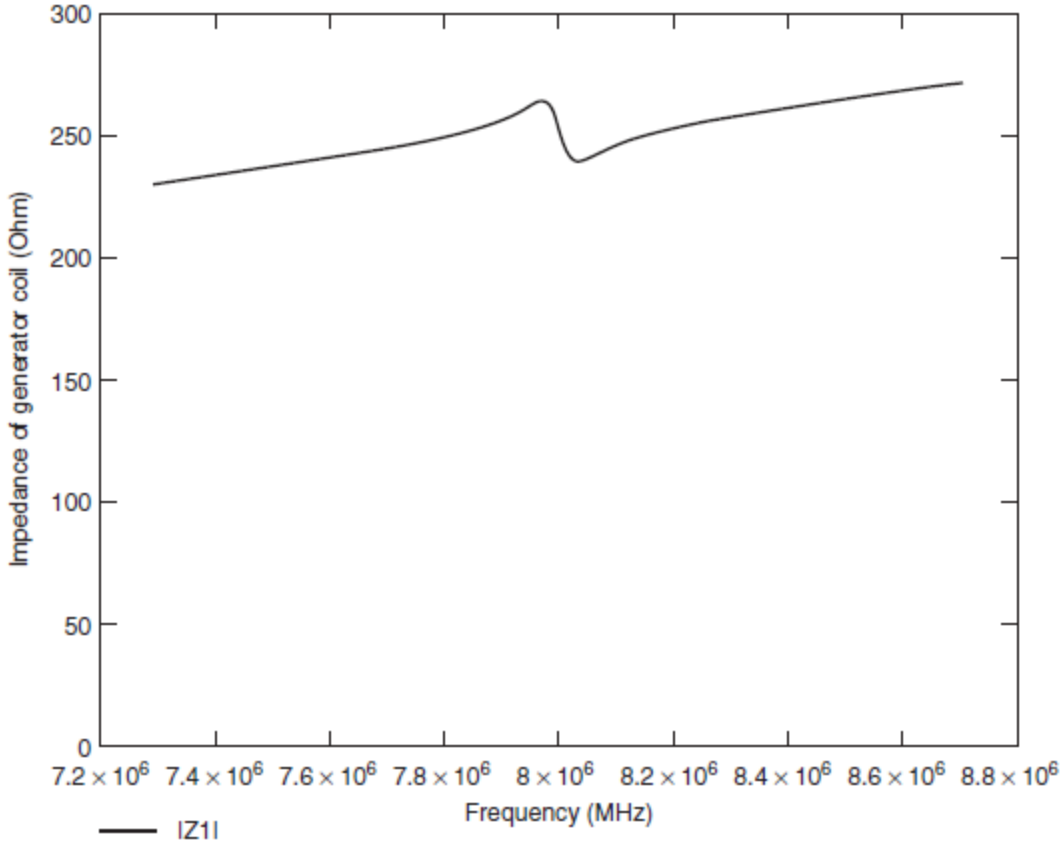
- No item data, just existence for warning
- Broadly adopted in clothes stores and libraries

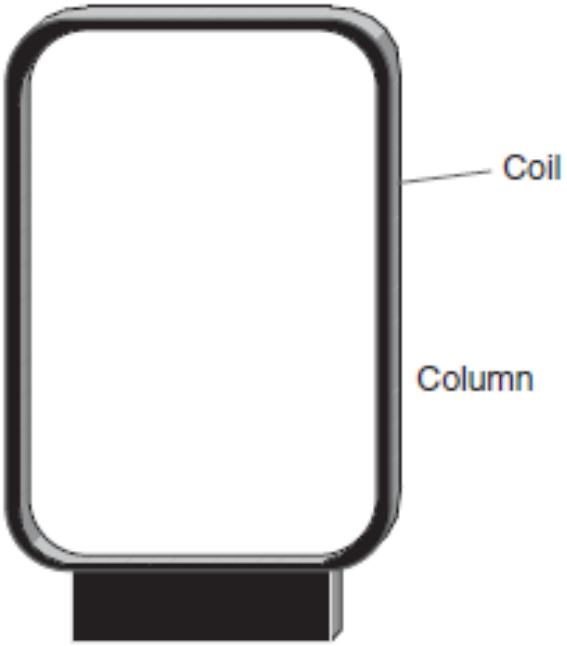
- One-time LC resonator
- 2^{nd} or sub-harmonic generation by diodes (RF)
- 2^{nd} or sub-harmonic generation by ferromagnetics (LF)

LC Resonator 1-Bit Transponder



LC Resonator 1-Bit Transponder

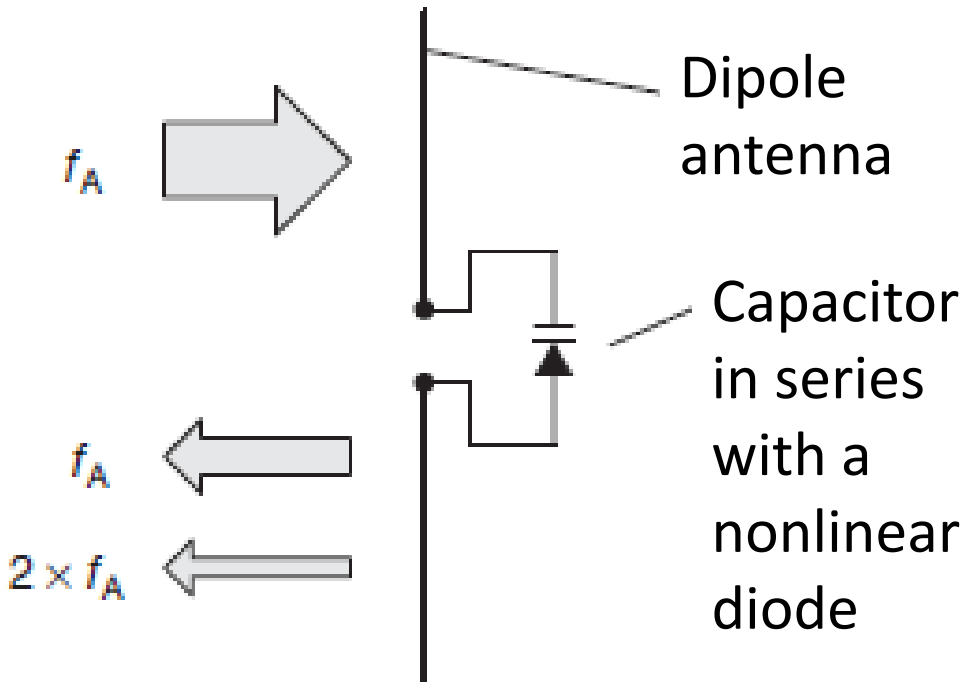


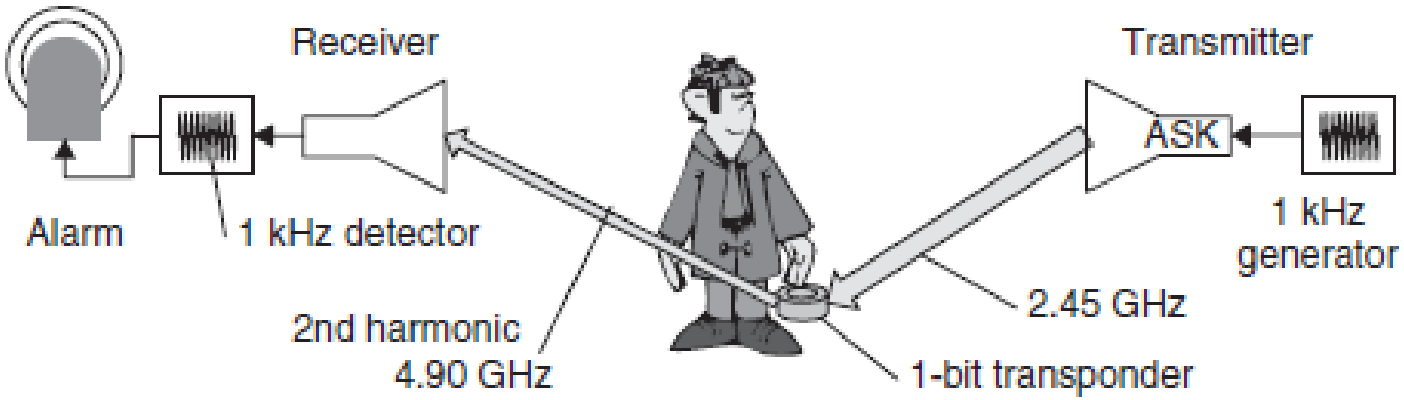


- Sweeping frequency to detect resonance: 7.4MHz – 8.8MHz
- Tags in close proximity and stronger field to break the capacitor for deactivation

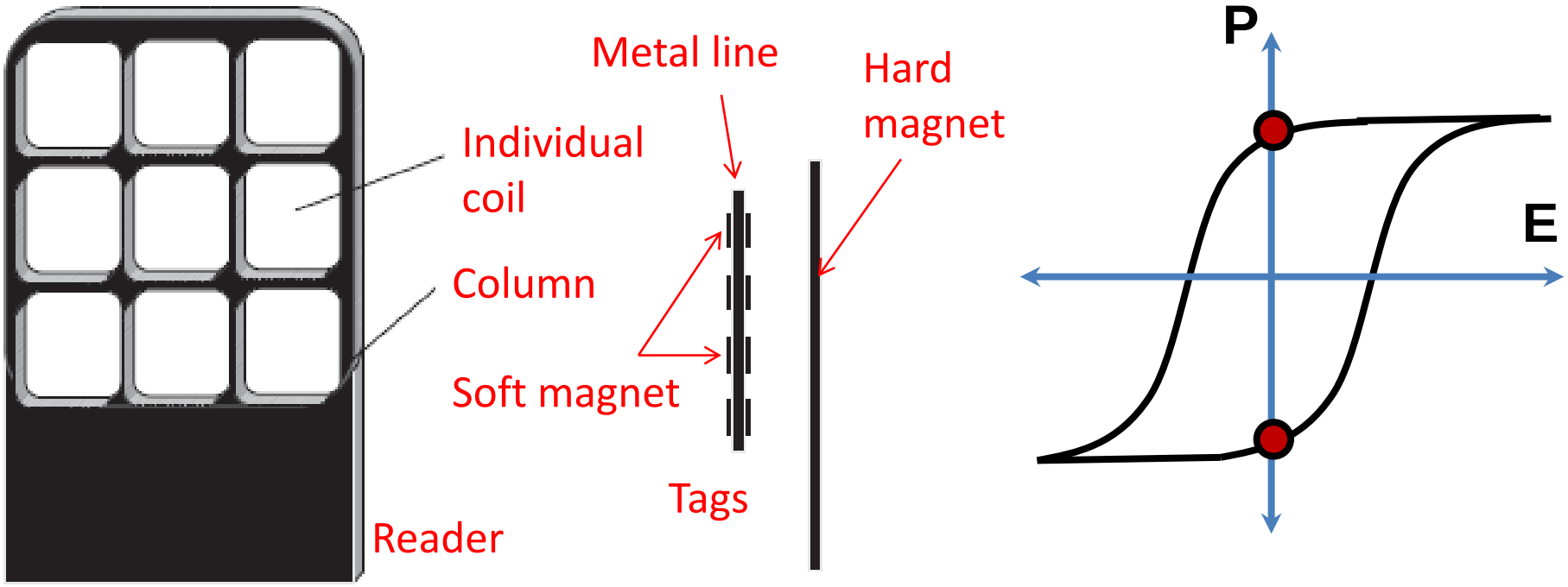
Microwave Harmonics 1-Bit Transponder

- f_A = 2.45GHz (ISM) and detection of 4.90 GHz.
- Usually f_A is modulated with a 1kHz coded signal, which will be reflected as the same 1kHz at 4.90 GHz after demodulation to reduce false positive.





Magnetic Strip 1-Bit Transponder



- Two frequencies impinges on the tag: f_1 = 3.5kHz and f_2 = 5.3kHz; the nonlinear P-E relation of a soft magnet around a metal line gives $f_1 + f_2$ = 8.8kHz and $f_1 - f_2$ = 1.8kHz to be detected.
- The hard magnet can be activated by a strong DC magnetic field to shield the soft magnet response, and can be reset with slow-decaying AC magnetic field.

Magnetic Strip 1-Bit Transponder

Group Exercise

- If we would to use RFID on tracking the bee population in a region…

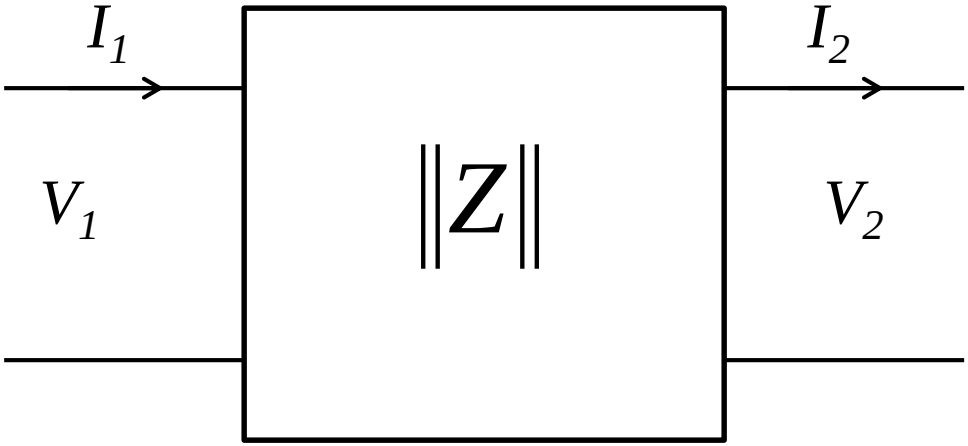
Outline

- Auto-ID system comparison
- Packaging and types of near-range reading
- The 1-bit transponder
- NFC RFID circuits

NFC Uses


Access control
Mobile payments
Loyalty programs
In-store marketing
Location-based services
Targeted marketing
Information exchange
Social networks
10:48
NFC
STARK
RFID

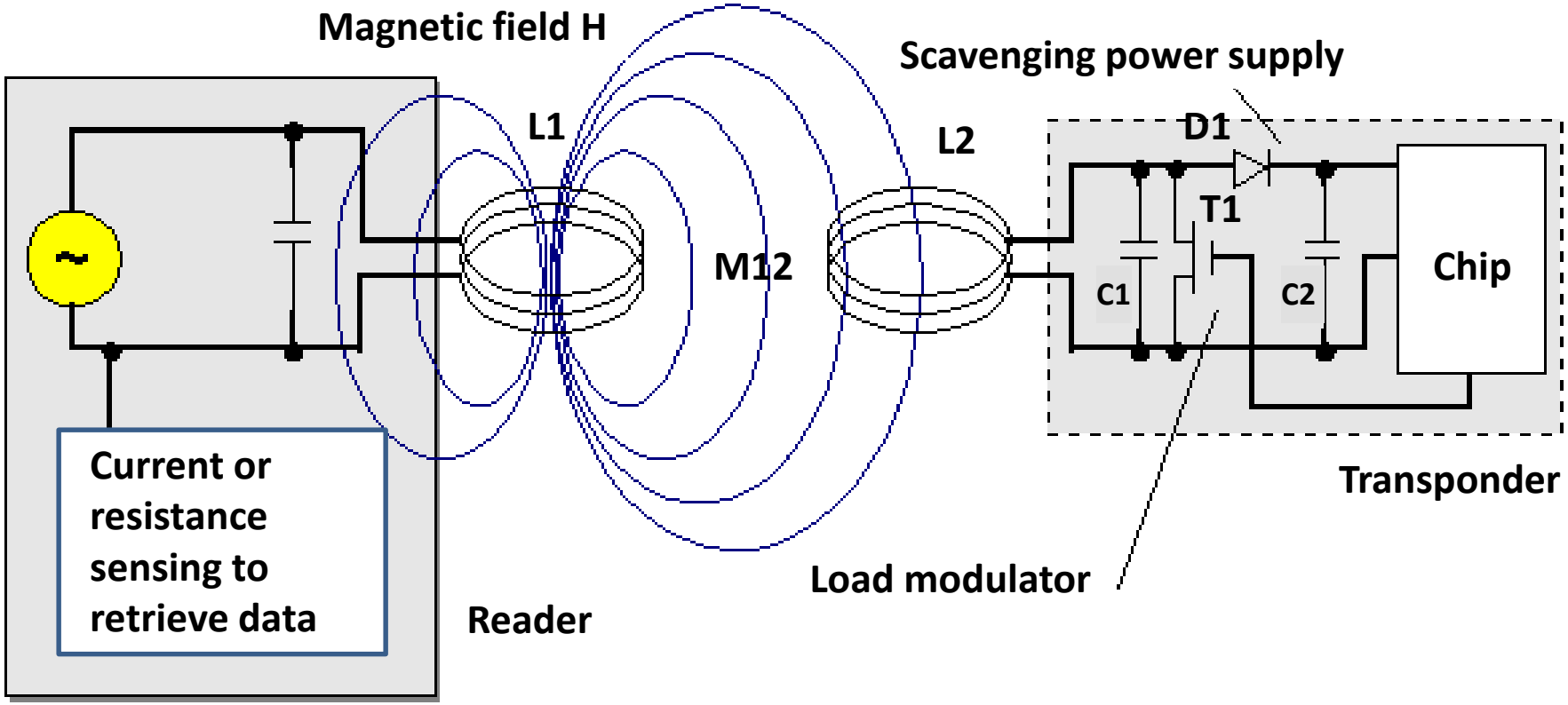
View of Transfer Function in Any Link



$$\begin{bmatrix} V_1 \\ I_1 \end{bmatrix} = \begin{vmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{vmatrix} \begin{bmatrix} V_2 \\ I_2 \end{bmatrix}$$

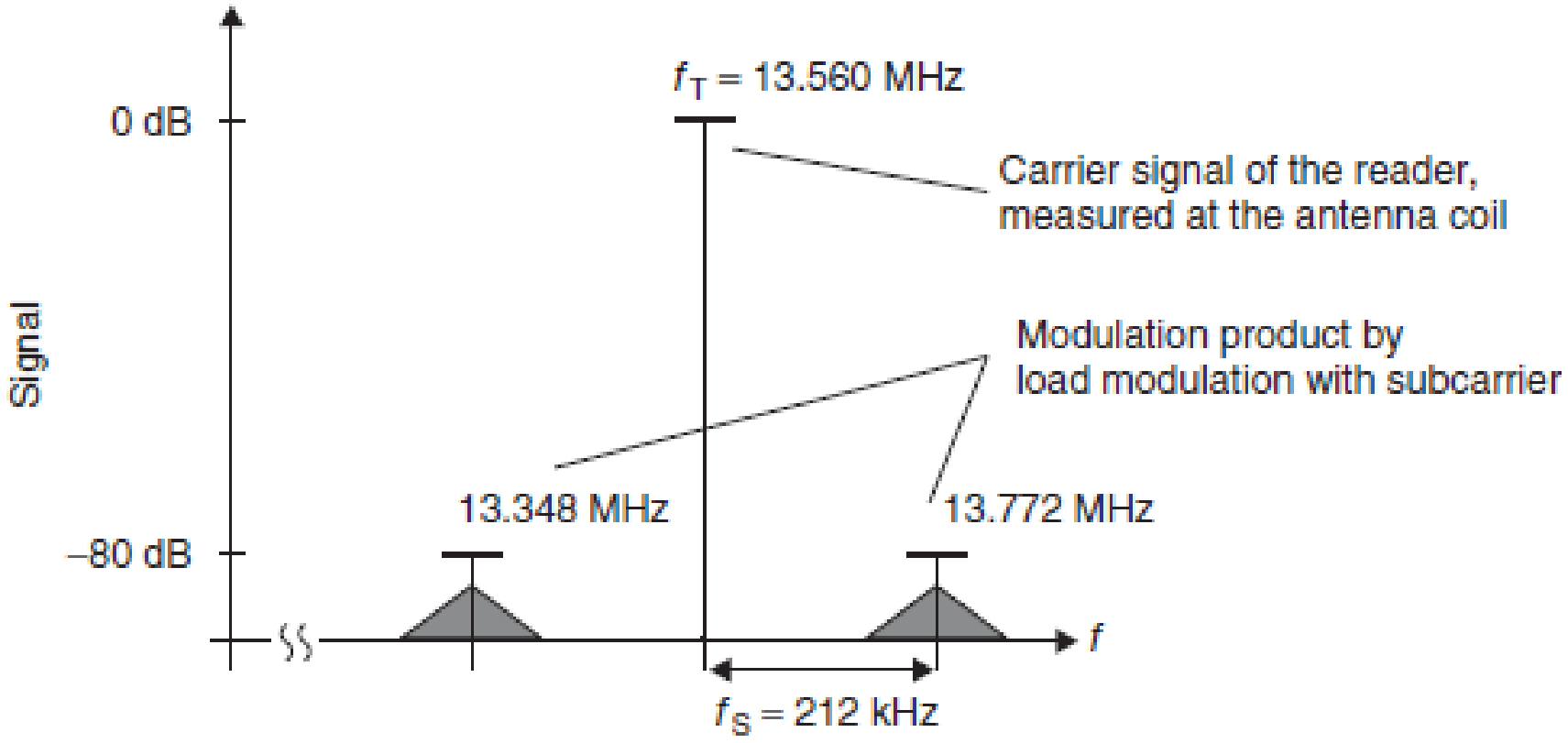
The transfer function of Z can represent signal links from NFC, UHF, transformer, etc.

NFC Inductive Load Coupling



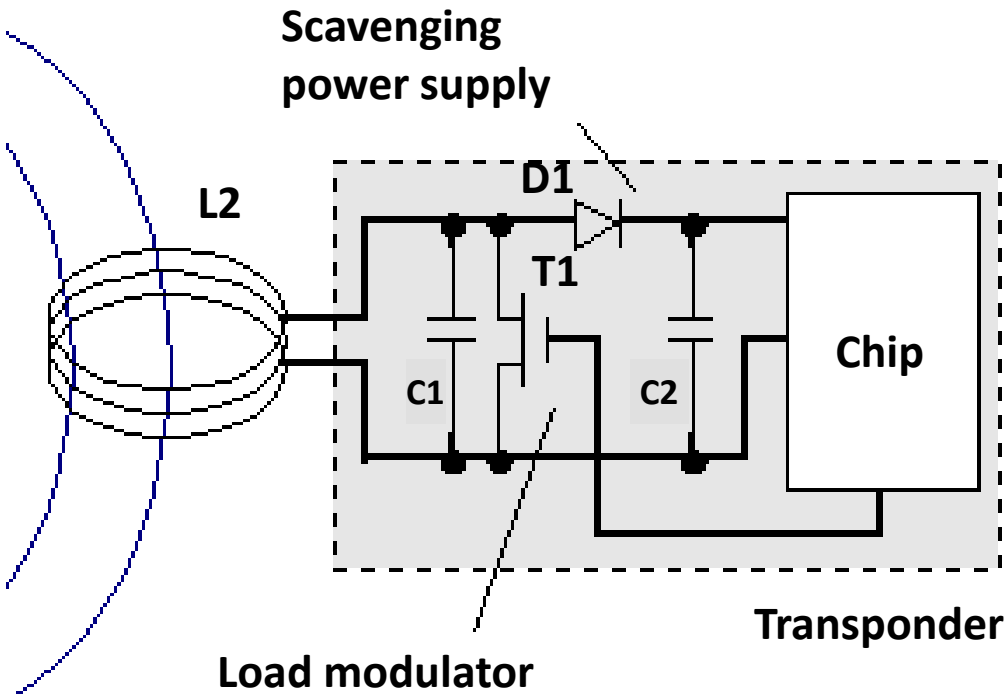
- Inductive load coupling is mostly by alternating magnetic fields.
- No constraint on quarter wavelength antenna in collecting radiating EM fields: just a transformer!
- Magnetic fields can be easily concentrated by ferromagnetic materials, and penetrate most materials well, including water.

NFC RFID Frequencies



- Load modulation presents very little need in bandwidth
- No multiplexing needed due to the short distance
- The reader can use a code injection to prevent eavesdropping

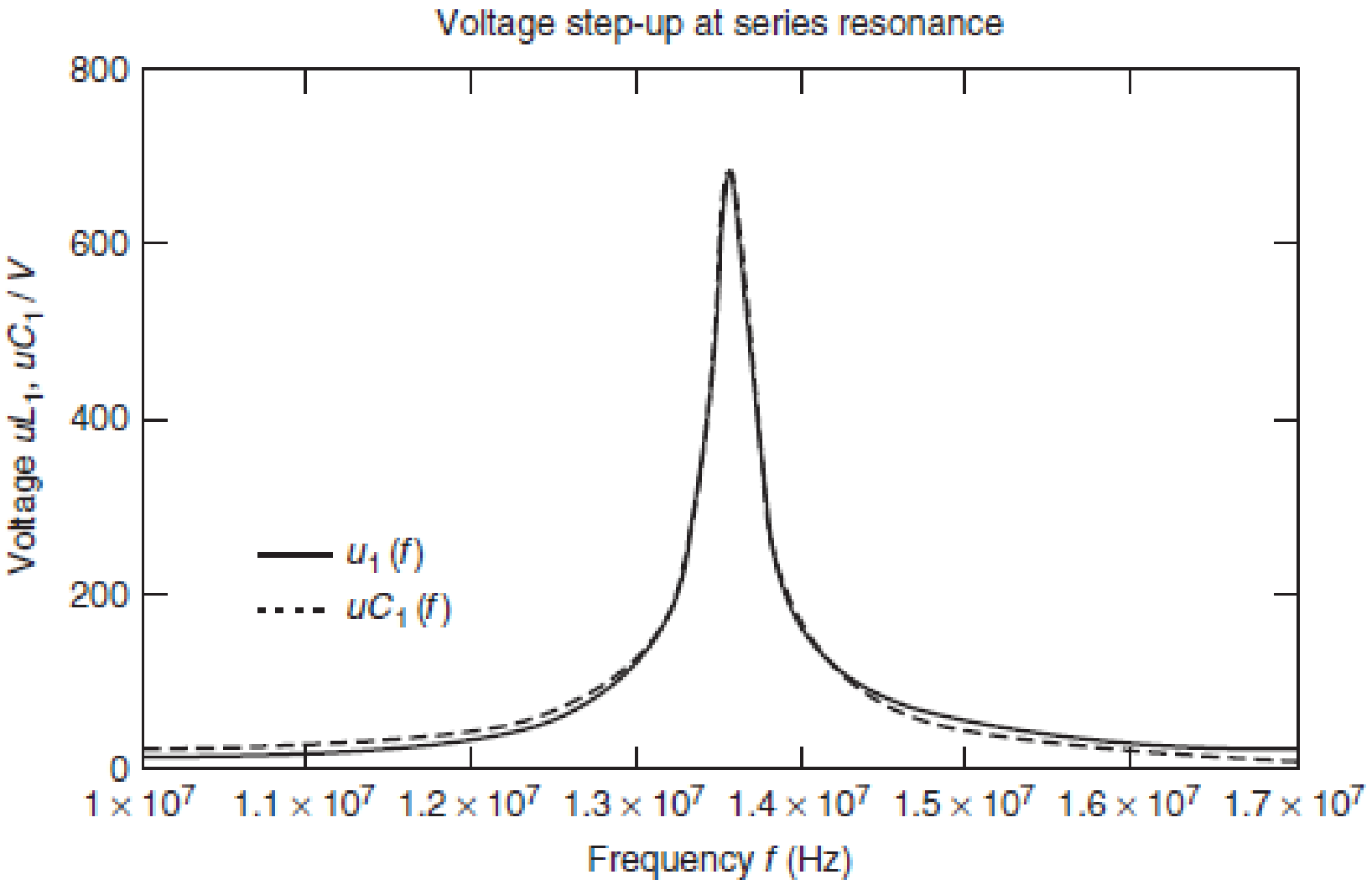
NFC Transponder Circuits



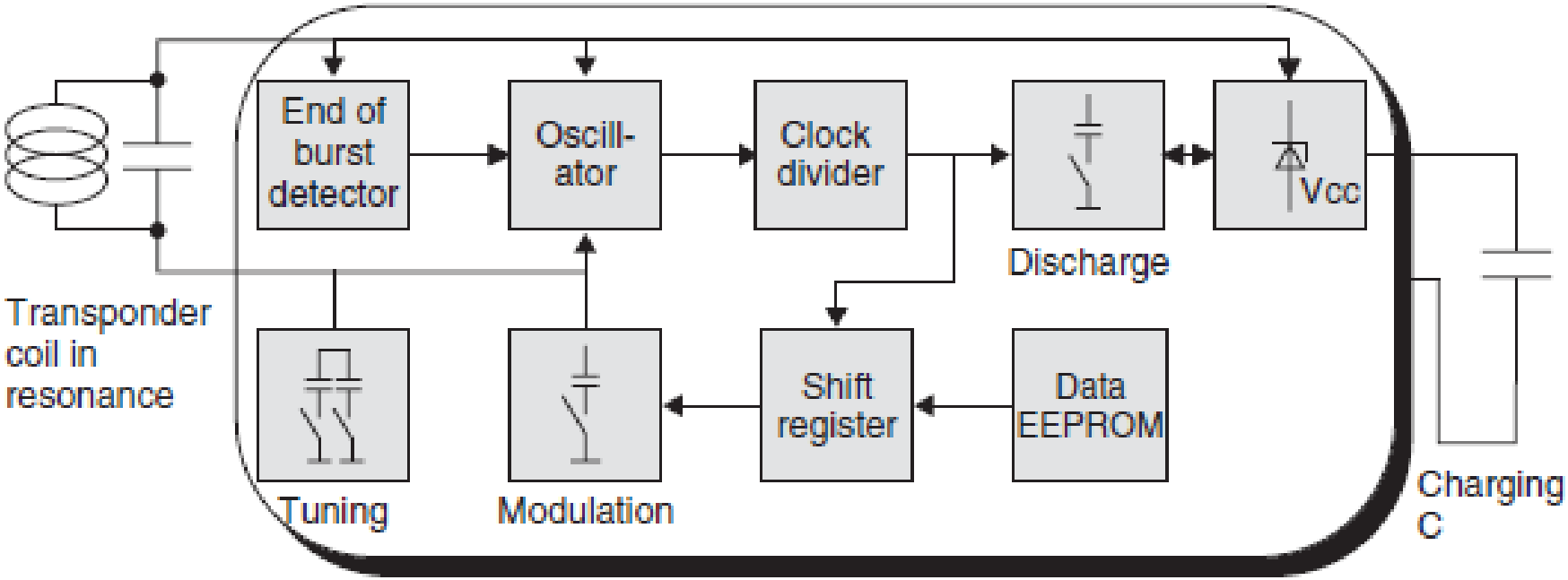
- The chip obtains the clock from the power line ripples (with frequency division)
- Voltage regulator for digital circuits
- ID bit-array storage
- Shifter to output the ID bits sequentially to T1

- L2 and C1 form the resonating circuits at the magnetic AC frequency to achieve the highest voltage at scavenging power supply.
- D1 and C2 form the rectifying and decoupling circuits for RF-to-DC conversion.
- T1 is often an RF transmission gate which modulates the load as seen from the current through L1 in the reader.

RF-to-DC Conversion at Resonance



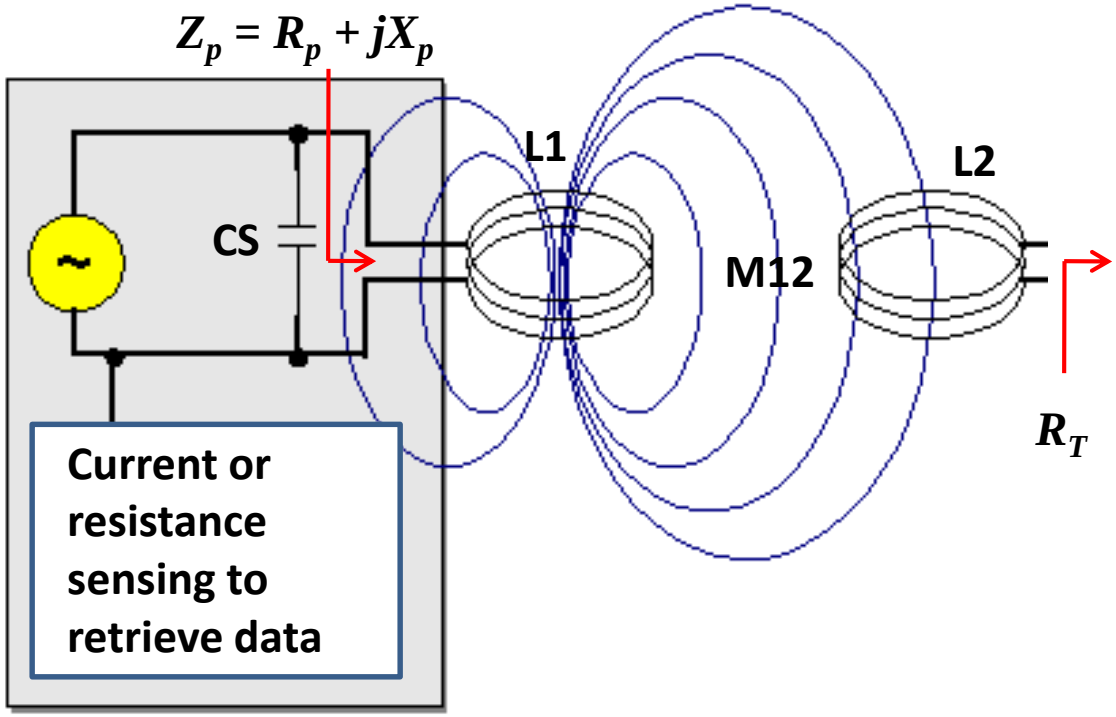
NFC Transponder Circuits



Texas Instrument TIRIS Transponder

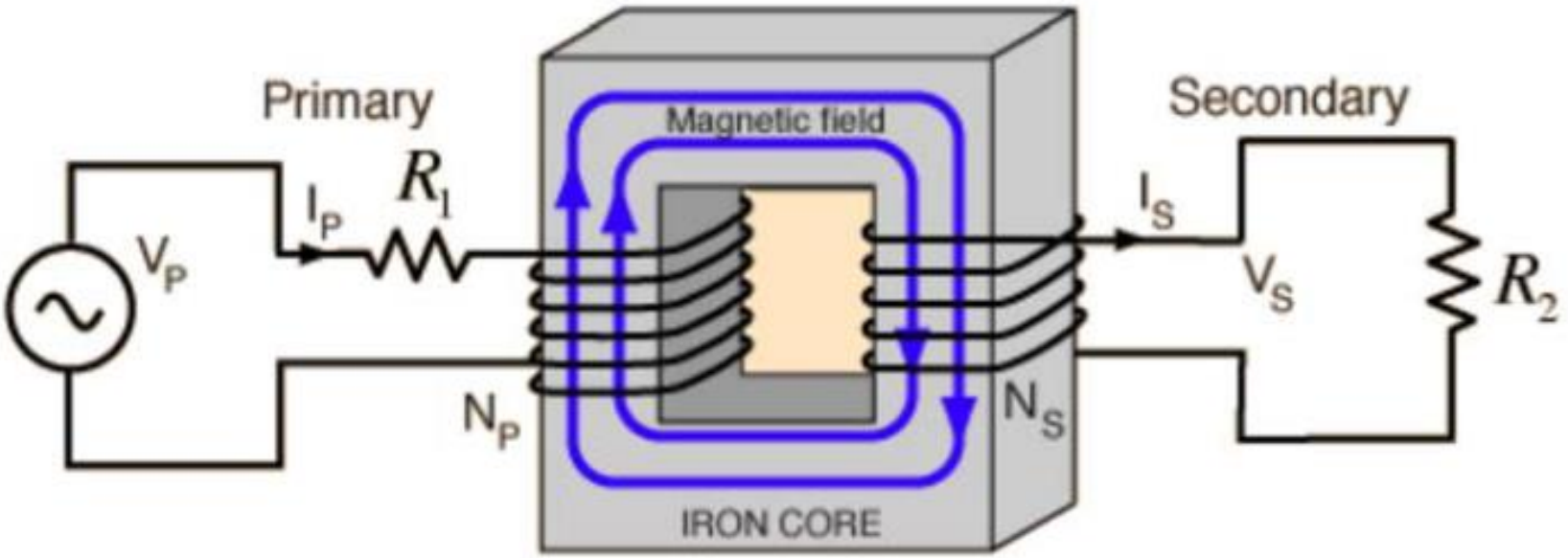
Note: TIRIS is an early example of transponder. With the superior TI switch capacitor technology in digital radio, FSK, instead of ASK or load modulation, controlled by the switch capacitor modulation is used.

NFC Inductive Coupling Circuits



- L1 and CS form a resonating circuit to deliver current through induction M12 to L2.
- The current in L2, or equivalently the source resistance, will be modulated by whether T1 presents as an open or short.
- M12 will be dominated by the magnetoresistive effect of the air.
- Most often L1 and L2 are in-plane low-Q coils to save cost

Transformer Circuit Analysis



$$V_P = I_P R_1 + L_1 \frac{dI_P}{dt} - M \frac{dI_S}{dt}$$

$$M \frac{dI_P}{dt} = I_S R_2 + L_2 \frac{dI_S}{dt}$$

$$M = k\sqrt{L_1 L_2}$$

k = 1 for loseless ferromagnetic coupling

Inductive Loading Impedance

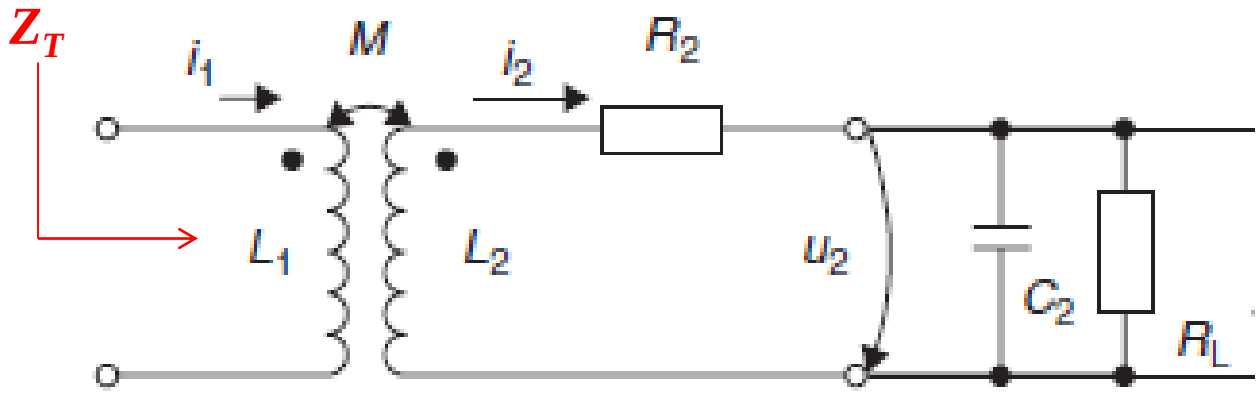
$$Z_P \equiv \frac{V_P}{I_P} = R_P + j\omega X_P$$

$$R_P = R_1 + \frac{\omega^2 M^2 R_2}{R_2^2 + \omega^2 L_2^2}$$

$$X_P = \omega L_1 - \frac{\omega^3 M^2 L_2}{R_2^2 + \omega^2 L_2^2}$$

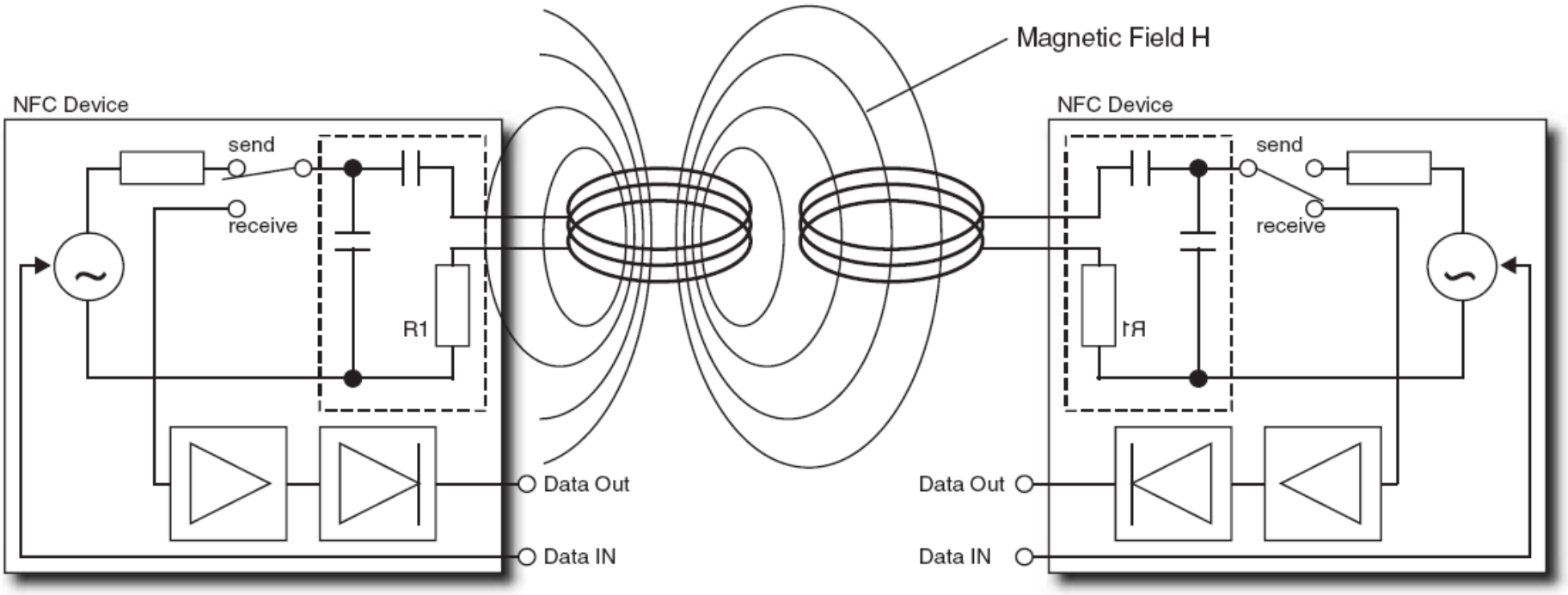
- If the resonance capacitance, diodes and switches are considered, the equation will be much more complicated.

Transformed Transponder Impedance



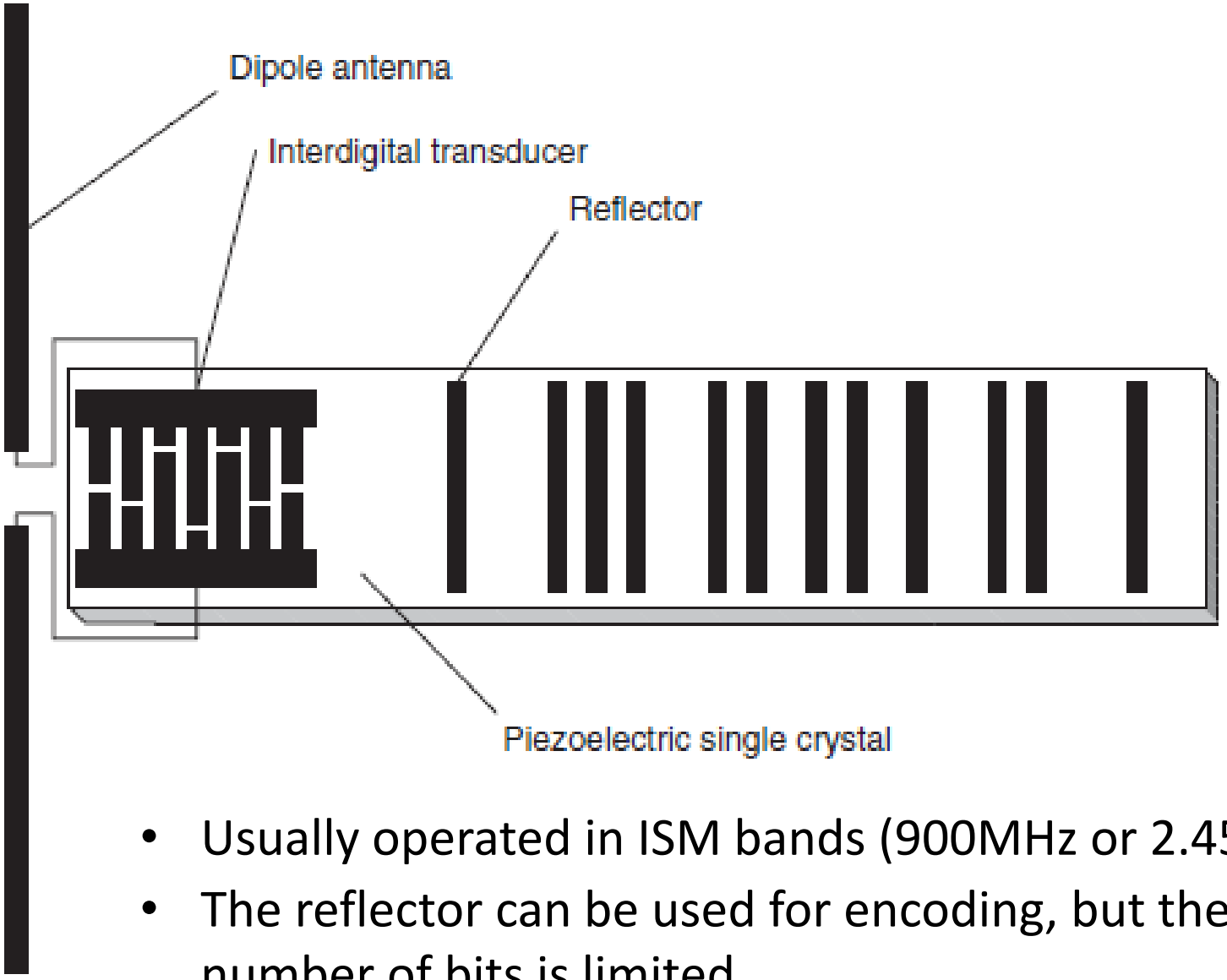
$$Z_T = \frac{\omega^2 k^2 L_1 L_2}{R_2 + j\omega L_2 + \dfrac{R_L}{1 + j\omega R_L C_2}}$$

Emulated NFC in the Active Mode



- Use of the NFC data protocol, two NFC readers can exchange data through SEQ or half-duplex “active” mode.
- Most cell phone OS support or will support NFC for both passive and active modes.

Other Possible Digital Transponders



- Usually operated in ISM bands (900MHz or 2.45GHz)
- The reflector can be used for encoding, but the number of bits is limited.

What Did You Learn

- Technology for near-range auto-ID
- Physical principles of near-range sensing
- Resonance and nonlinearity for 1-bit transponder
- Transformer circuits for NFC RFID