UNIVERSITÄT OSNABRÜCK

Wireless Medium Access Technologies

ZigBee & RFID

Mobile Communication, WS 2014/2015, Kap.3.4

Prof. Dr. Nils Aschenbruck

3.4.1 IEEE 802.15.4 – ZigBee

Due to the limited device capabilities, **IEEE 802.11** is usually **unsuitable** for sensor network applications, because it requires

- too many computational resources
- too much energy for transmitting and receiving.

An alternative is **IEEE 802.15.4**, also called **Zigbee**:

- specially designed for sensor network applications
- tailored towards **long lifetime**
- provides low data rates
  - sufficient for many applications
- **multi-hop networks** already supported in the standard
- special PHY layers for special purposes
  - e.g. Chirp Spread Spectrum
  - provides **robustness** and location services

WSN Application Scenarios

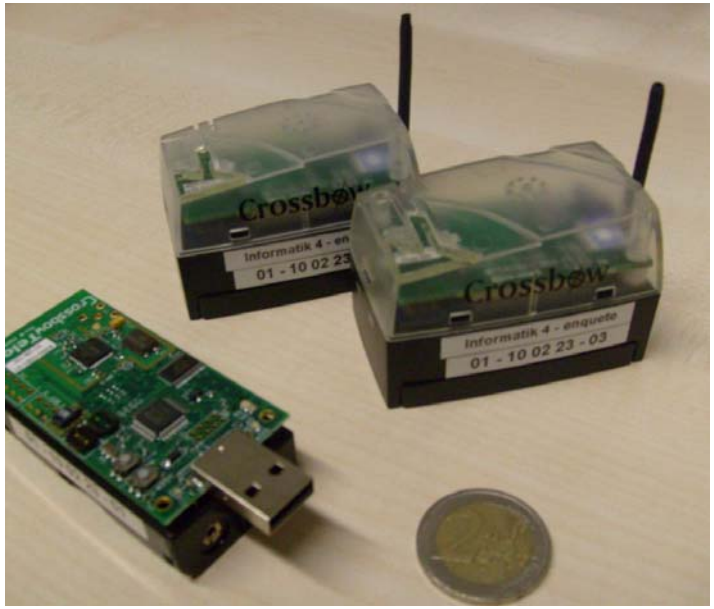

wikipedia.org by Goldlocki


wikipedia.org by DAR56

Scenarios

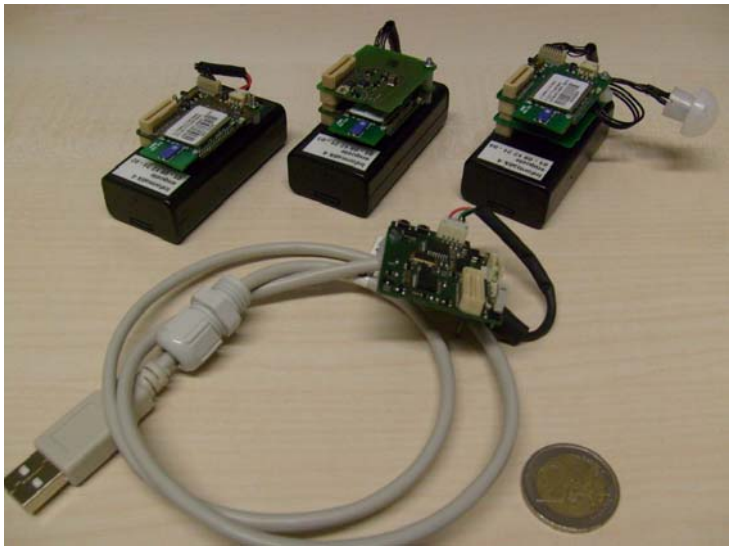
WSN Application Scenarios

Sallai et al.: “Acoustic Shooter Localization with a Minimal Number of Single-Channel Wireless Sensor Nodes” in Proceedings of SenSys 2011.



Crossbow/Memsic Hardware

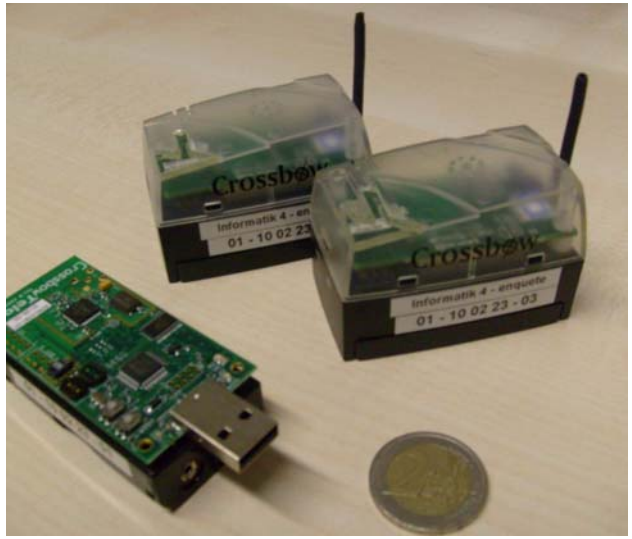
- Mote platform MPR2600/IRIS for basic functionality
- Sensor data acquisition board MTS420
  (accelerometer, light sensor, barometer, thermometer, humidity sensor, GPS receiver)
- Gateway MIB520 as interface to PC via USB
- Research platform TPR2420/TelosB
  (light sensor, thermometer, humidity sensor)



iSense Hardware

- modular hardware platform for combining multiple sensor modules
- core module
  - provides basic sensor functionality (OS, software)
  - CPU, clock, RAM, flash memory, radio
- environment module (thermometer, light sensor)
- security module (infrared sensor, accelerometer)
- gateway module: interface between sensor network and PC via USB

WSNs – Just to be on the same page...



Resource Constrains

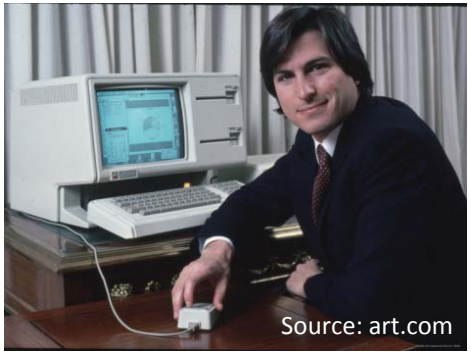
- Memory (e.g., 1024 kB ROM + 10 kB RAM)
- Processing Power (e.g., 8-16 MHz)
- Battery-driven

Plattform	TelosB	MicaZ	GNodes
MPU	MSP430	ATmega128L	MSP430
	8 MHz 16 bit	8 MHz 8 bit	16 MHz 16 bit
ROM	48 kB	128 kB	116 kB
RAM	8 kB	4 kB	8 kB
Flash	1024 kB	512 kB	1024 kB
Radio	CC2420 AES support 250 kbps	CC2420 AES support 250 kbps	CC1101 38,4 kbps
Frequenz	2,4 GHz	2,4 GHz	868 MHz

… compare it to something we all know …

IBM PC (1981)

- ~5 MHz, 16 Bit
- 16/64 kB RAM
- HDD 10MB (later versions)



Apple Macintosh (1984)

- 8 MHz
- 128 kB RAM

Amiga 500 (1987)

- ~8 MHz, 16 Bit
- 512 kB RAM

Plattform	TelosB	MicaZ
MPU	MSP430	ATmega128L
	8 MHz 16 bit	8 MHz 8 bit
ROM	48 kB	128 kB
RAM	8 kB	4 kB
Flash	1024 kB	512 kB
Radio	CC2420 AES support 250 kbps	CC2420 AES support 250 kbps
Frequenz	2,4 GHz	2,4 GHz

IEEE 802.15.4 – Features

IEEE 802.15.4-2006 is a standard which specifies the **physical layer** and **media access control** for low-rate wireless personal area networks (LR-WPANs).
It is the basis for the **ZigBee**, WirelessHART, and MiWi specification, each of which further attempts to offer a complete networking solution by developing the upper layers which are not covered by the standard.

Features IEEE 802.15.4

- Data rates of 250 kbps, 40 kbps, and 20 kbps.
- Two addressing modes; 16-bit short and 64-bit IEEE addressing.
- Support for critical latency devices, such as joysticks.
- **CSMA-CA** channel access.
- Automatic network establishment by the **coordinator**.
- Fully handshaked protocol for transfer reliability.
- Power management to ensure **low power consumption**.
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz and one channel in the 868MHz band.

IEEE 802.15.4


IEEE 802.15.4 - Konqueror
Location Edit View Bookmarks Tools Settings Help
http://www.ieee802.org/15/pub/TG4.html
Google Search
IEEE 802.15.4
search
WPAN Home Page
IEEE Wireless Zone
IEEE 802.11 WLAN
IEEE 802.16 WMAN
IEEE 802.18
Regulatory
IEEE 802 LMSC
IEEE-SA
IEEE-ISTO
IEEE
IEEE 802.15 WPAN™ Task Group 4 (TG4)
Sunday, 7 February 2010
The IEEE 802.15 TG4 was chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.
IEEE 802.15 TG4 OFFICERS CONTACT INFORMATION
Chair: Pat Kinney
Vice Chair: Phil Jamieson
Technical Editor: Jose Gutierrez
Secretary: Marco Naeve
IEEE 802.15 TG4 CURRENT STATUS
The IEEE 802.15.4-2003 standard has been superceded by the publication of IEEE 802.15.4-2006. The new standard can be purchased from the IEEE store. The TG4 task group put itself into hibernation at the March 2004 meeting after forming a task group (TG4b). The new task group 4b completed is work with the publication of the revision. Additional information can be found on the TG4b web site.
To get more information on TG4 and how to get involved check the TG4 Expert web site.
IEEE 802.15 TG4 FEATURES
Data rates of 250 kbps, 40 kbps, and 20 kbps.
Two addressing modes; 16-bit short and 64-bit IEEE addressing.
Support for critical latency devices, such as joysticks.
CSMA-CA channel access.
Automatic network establishment by the coordinator.
Fully handshaked protocol for transfer reliability.
Power management to ensure low power consumption.
16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz I and one channel in the 868MHz band.
IEEE 802.15 TG4 MAILING LIST
Major announcements related to TG4 will be published on the 802.15.4 TG4 Public Mailing List <stds-802-15-4@ieee.org>.
You can learn more about the 802.15 Mailing Lists by pointing your browser here.
The WG Mailing Lists are converted into an HTML mail archive which can be sorted by subject & date.
Page loaded

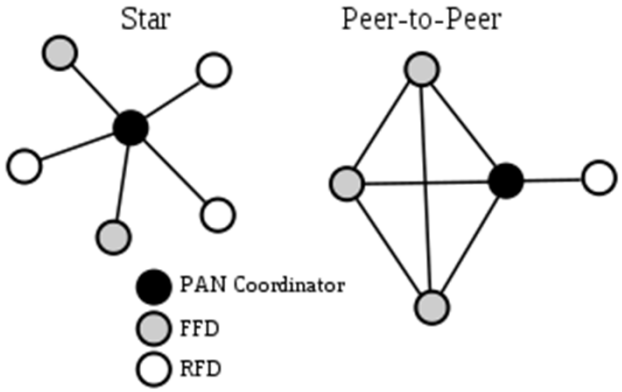
IEEE 802.15.4 – Node Types and Topologies

Full-function device (FFD)

- can serve as the coordinator
- may relay messages
- every network needs at least one FFD

Reduced-function devices (RFD)

- extremely simple devices
- can only communicate with FFD's
- can never act as coordinators.



Peer-to-peer (or point-to-point) Topologies

- arbitrary patterns of connections
- extension is only limited by the distance between each pair of nodes
- cluster-tree topologies special kind using cluster heads

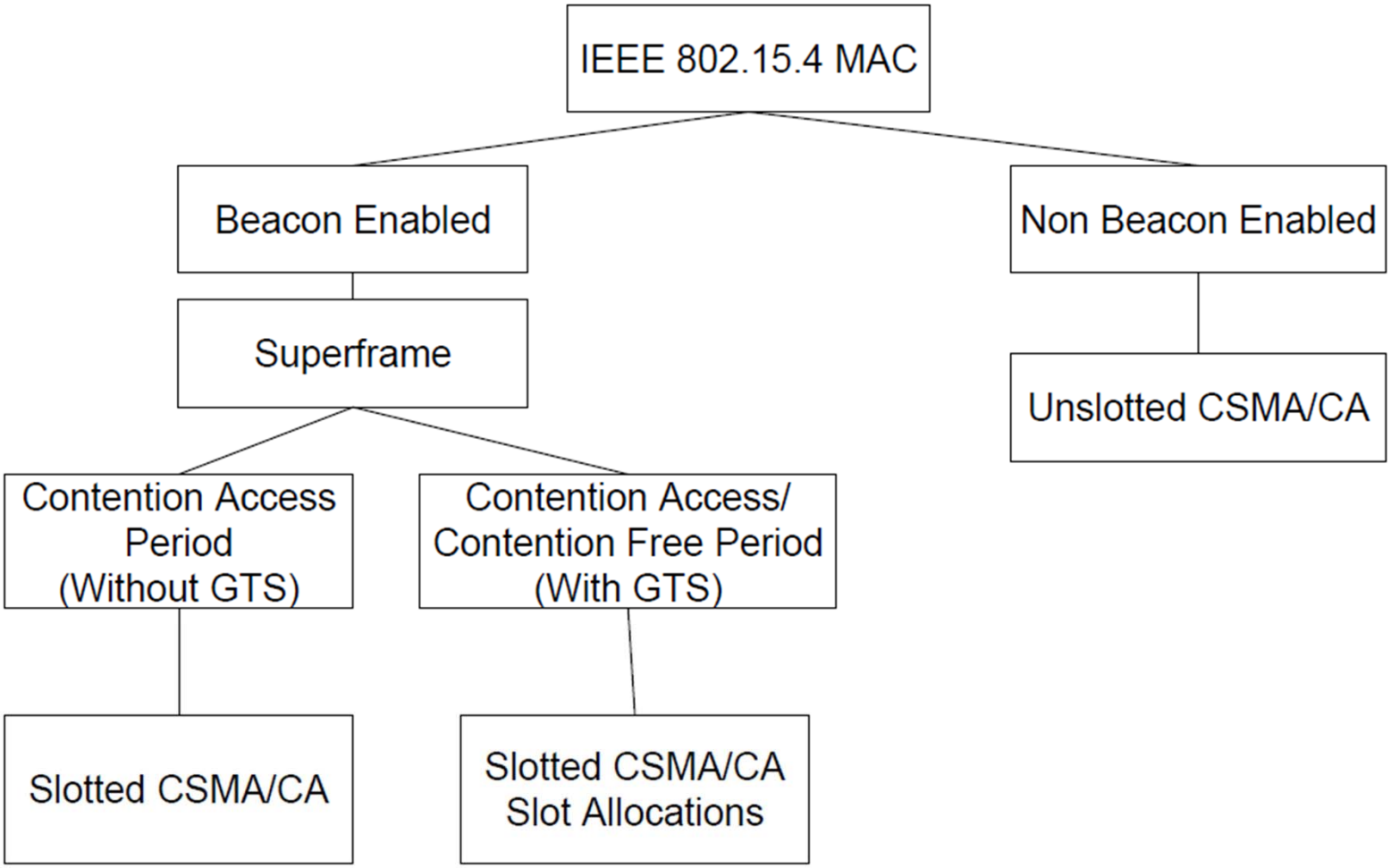
Star Topologies

- the coordinator of the network will necessarily be the central node

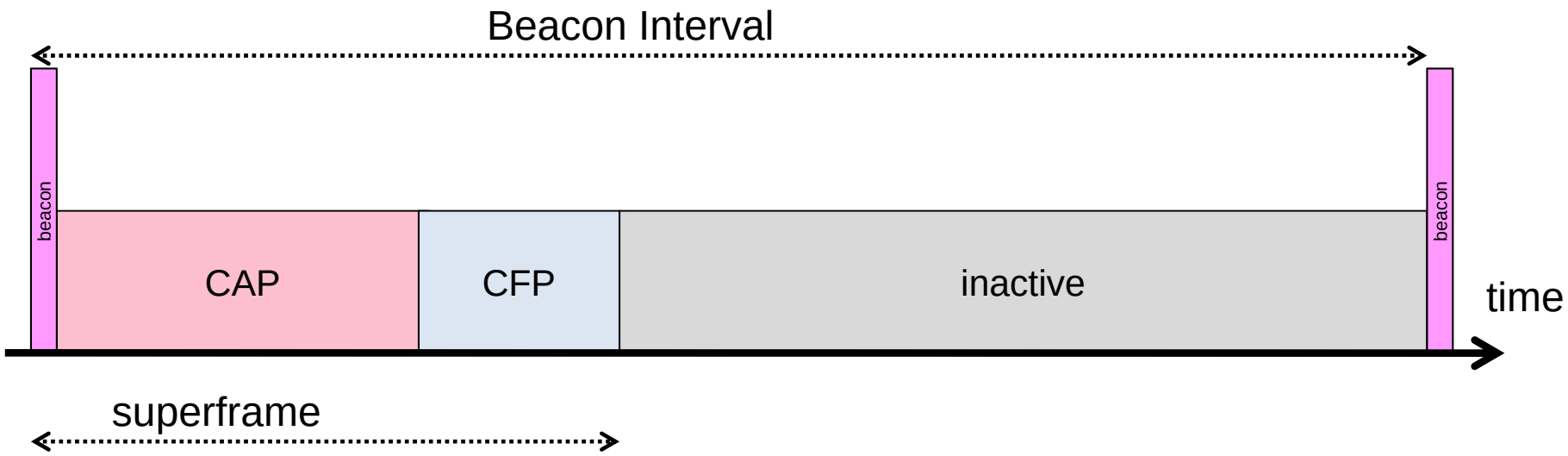
IEEE 802.15.4 – Channel Access

- non beacon-enabled mode
  - simple non-slotted CSMA/CA
- beacon-enabled mode
  - PAN coordinator sends beacons
  - nodes synchronize using this beacons
  - slotted CSMA/CA
  - Guaranteed Time Slots (GTS) for real-time
  - nodes may sleep between beacons
    - either they have data to send
    - or the beacon tells them to listen
    - or they may sleep

IEEE 802.15.4 – Channel Access



IEEE 802.15.4 – Channel Access



CAP – Contention Access Period

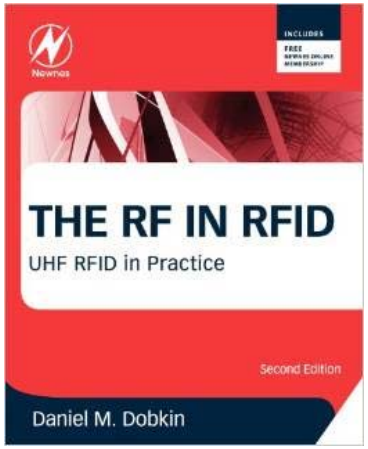
CFP – Contention Free Period
including Guaranteed Time Slot (GTS)

3.4.2 RFID

- since WW2: Identification Friend or Foe (IFF)
- radar technology

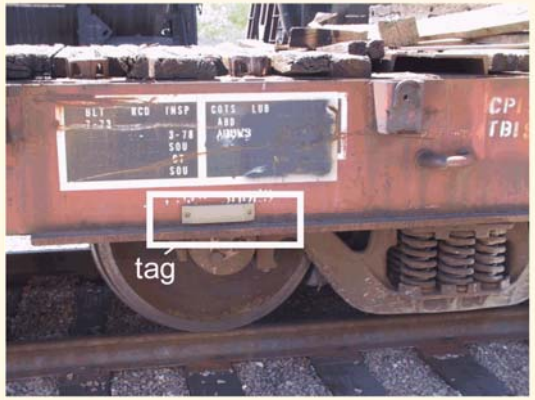
Literature:

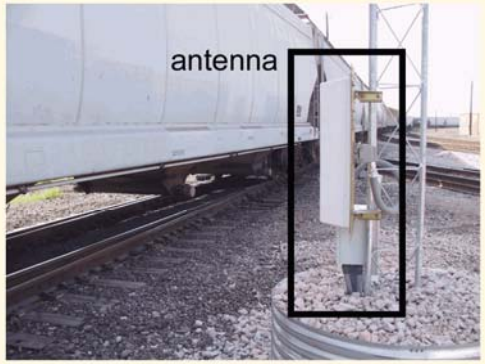
- Daniel M. Dobkin: “The RF in RFID, Second Edition: UHF RFID in Practice”, Newnes, 2 ed., 2012
- Daniel M. Dobkin: “Quick Introduction to RFID”, http://www.polygait.calpoly.edu/tutorial.htm
- EPCglobal UHF Class 1 Gen 2 Standard: “EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID - Specification for RFID Air Interface - Protocol for Communications at 860 MHz – 960 MHz”, Version 2.0.0, Nov. 2013, http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2



RFID Applications

Source: Dan Dobkin "Quick Introduction to RFID", http://www.polygait.calpoly.edu/tutorial.htm

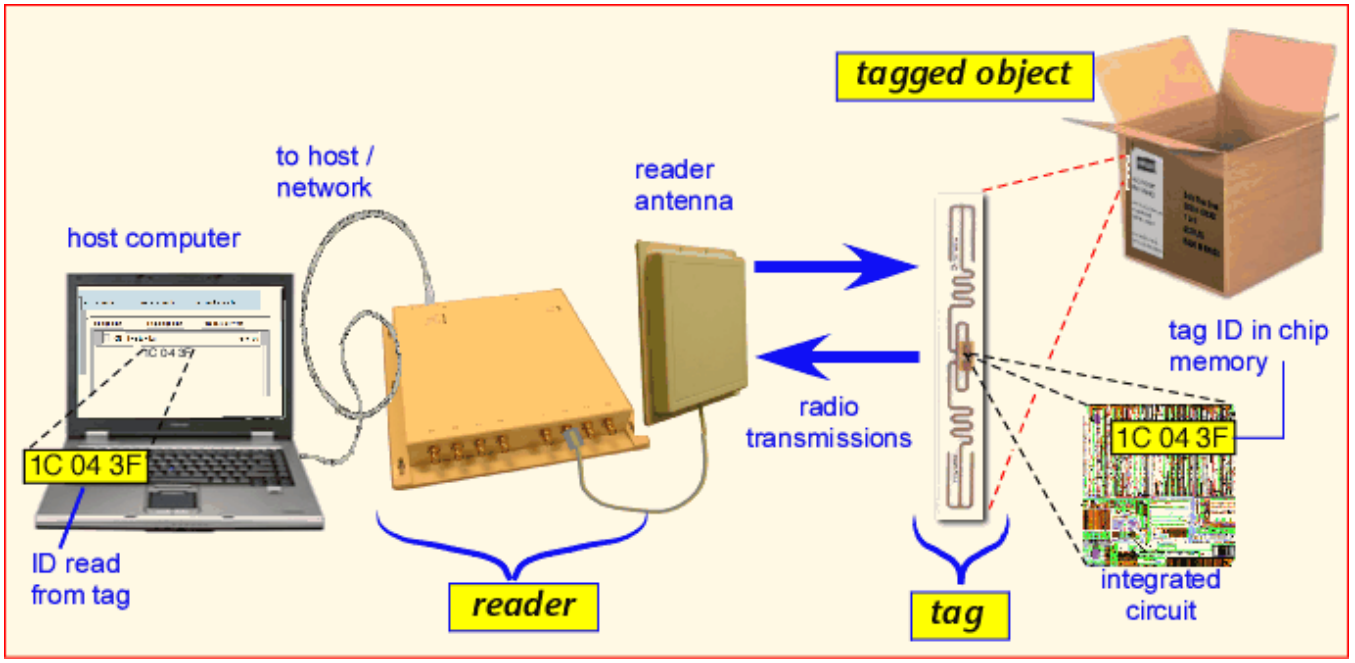




images courtesy Andrew Friend, ATBD Inc.

Source: R. Anson Eaglin, USDA NAIS Strategic Plan 4/05

RFID – Setup



Source: Dan Dobkin "Quick Introduction to RFID", http://www.polygait.calpoly.edu/tutorial.htm

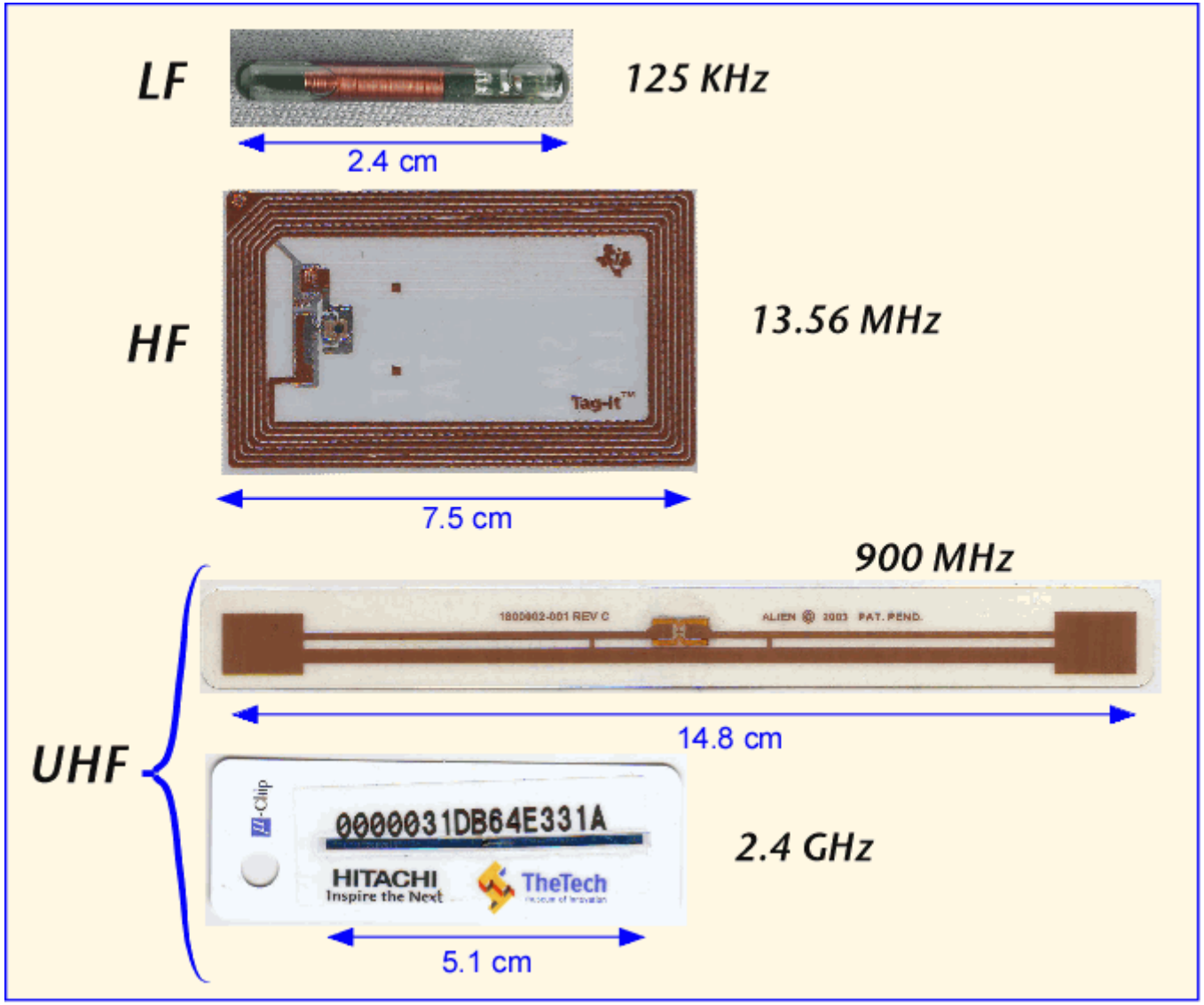
Types of RFID

	Typ. Frequenzen	Typ. maximale Reichweite (Tag passiv)	Typ. Anwendungen
Low Frequency (LF)	**125/134 kHz**	**< 1 m**	• **Tier-Identifizierung** • **Zugangskontrolle**
High Frequency (HF)	**13,56 MHz**	**< 1 m**	• **Bargeldloses Bezahlen** • **Smart-Cards** • **Near Field Communication (NFC)**
Ultra High Frequency (UHF)	**860 – 960 MHz**	**2 – 10 m**	• **Logistik (EPCglobal C1 G2)**
UHF „Microwave“	**2,4 – 2,45 GHz**	**1 – 3 m**	• **Logistik (kleinere Tags)**

Vgl.: Daniel M. Dobkin, “The RF in RFID – UHF RFID in Practice”

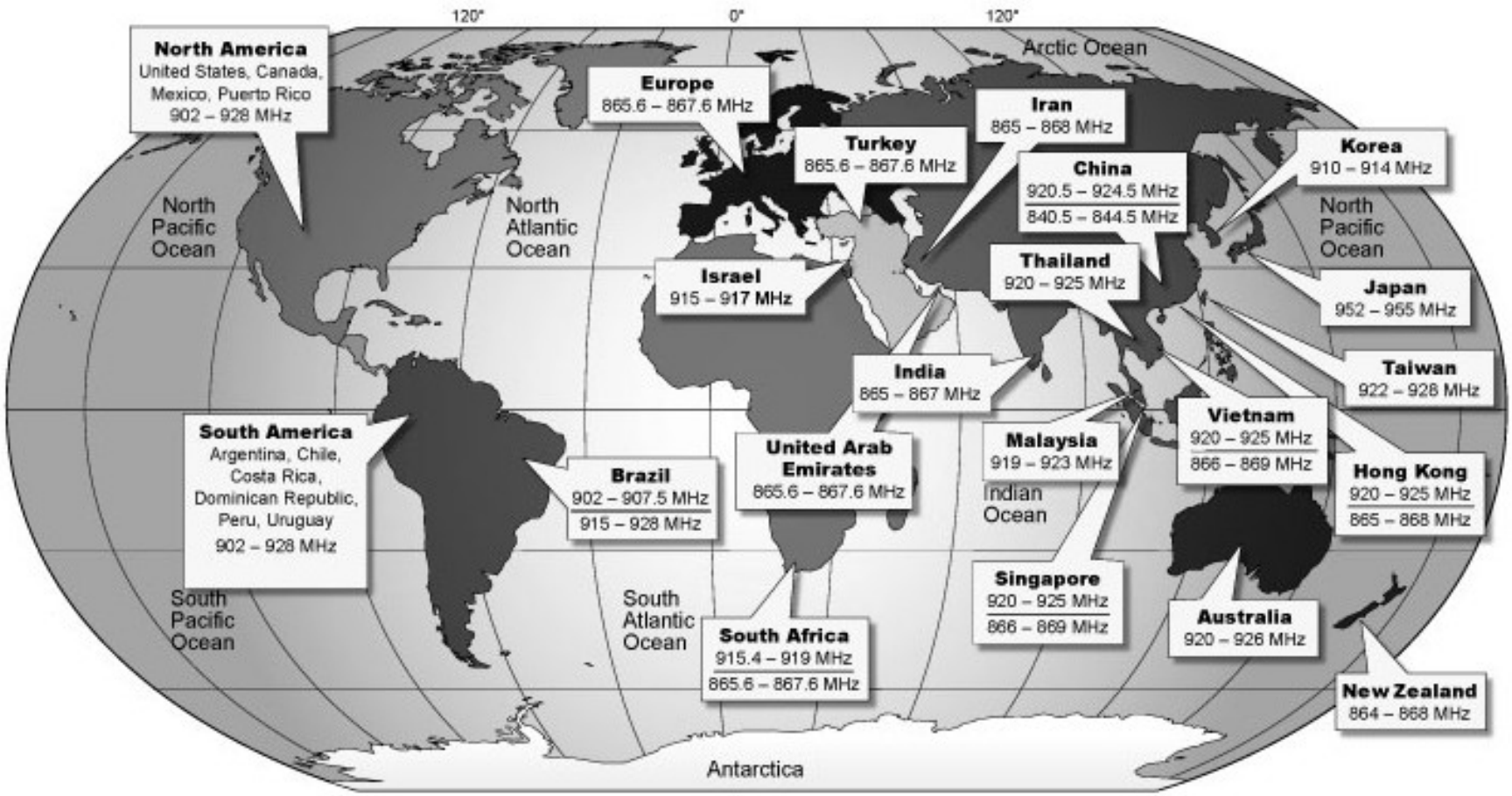
- *Actual range depends on different factors:*
  - Reader: transmission power, antenna(s)
  - Tag: antenna
  - Environment: small scale fading: interference, multi-path effects, …
  - ….

Types of RFID (2)



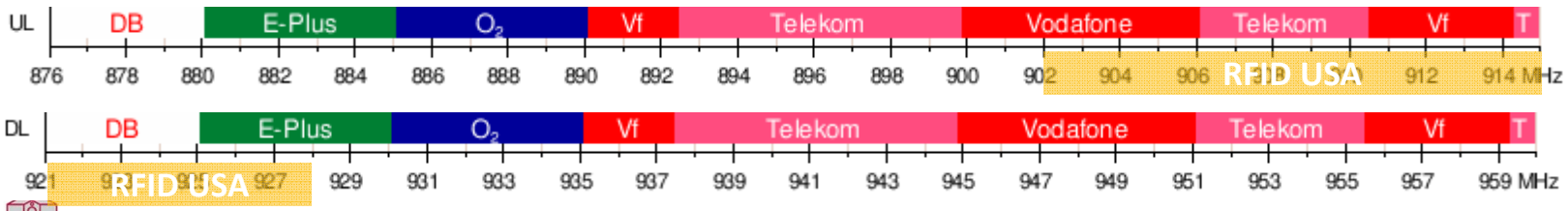
Source: Dan Dobkin "Quick Introduction to RFID", http://www.polygait.calpoly.edu/tutorial.htm

Bands available for UHF-RFID use in the 860-960 MHz range



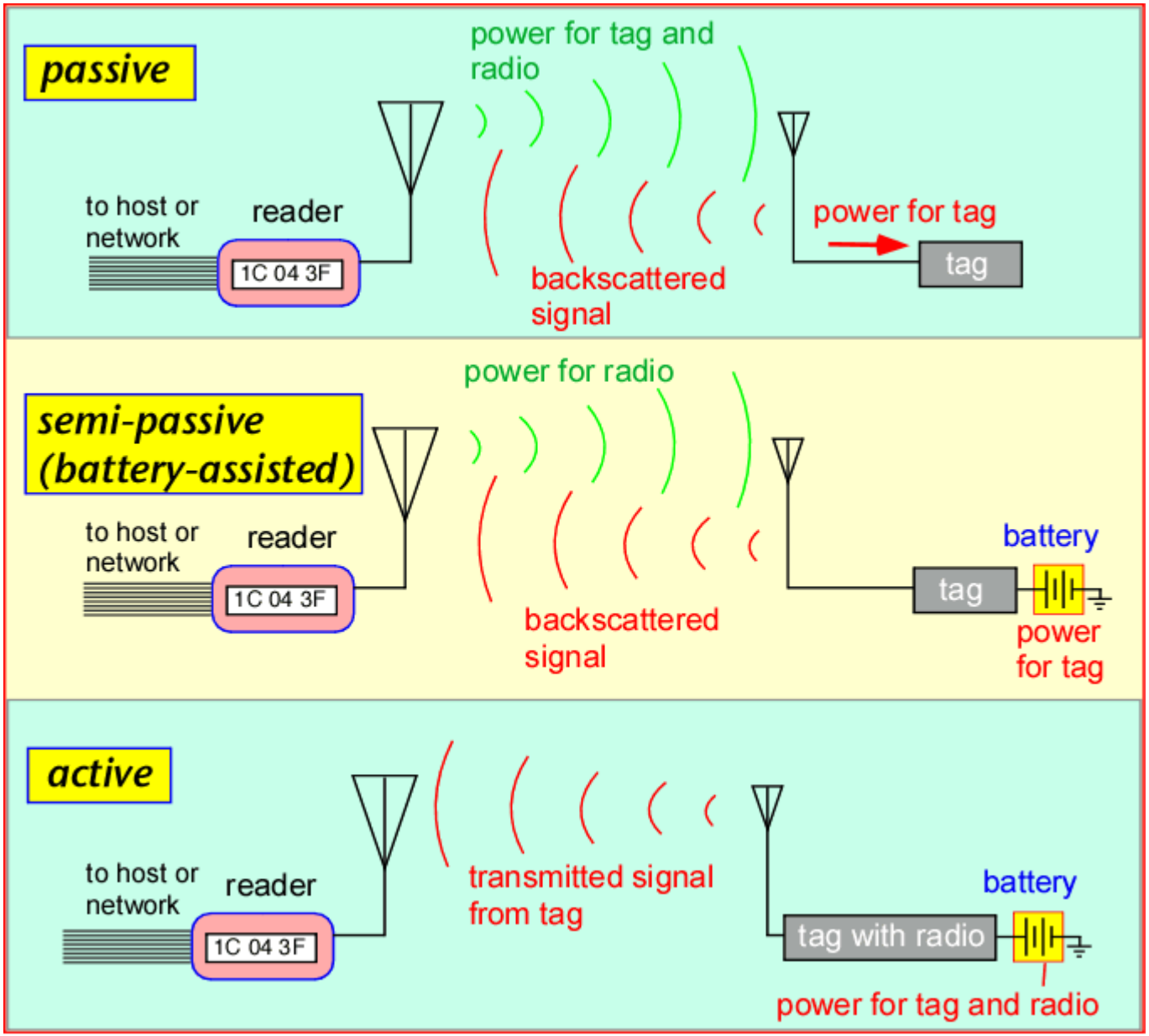
Source: assettrackit.com

GSM 900 Germany



Source: de.wikipedia.de

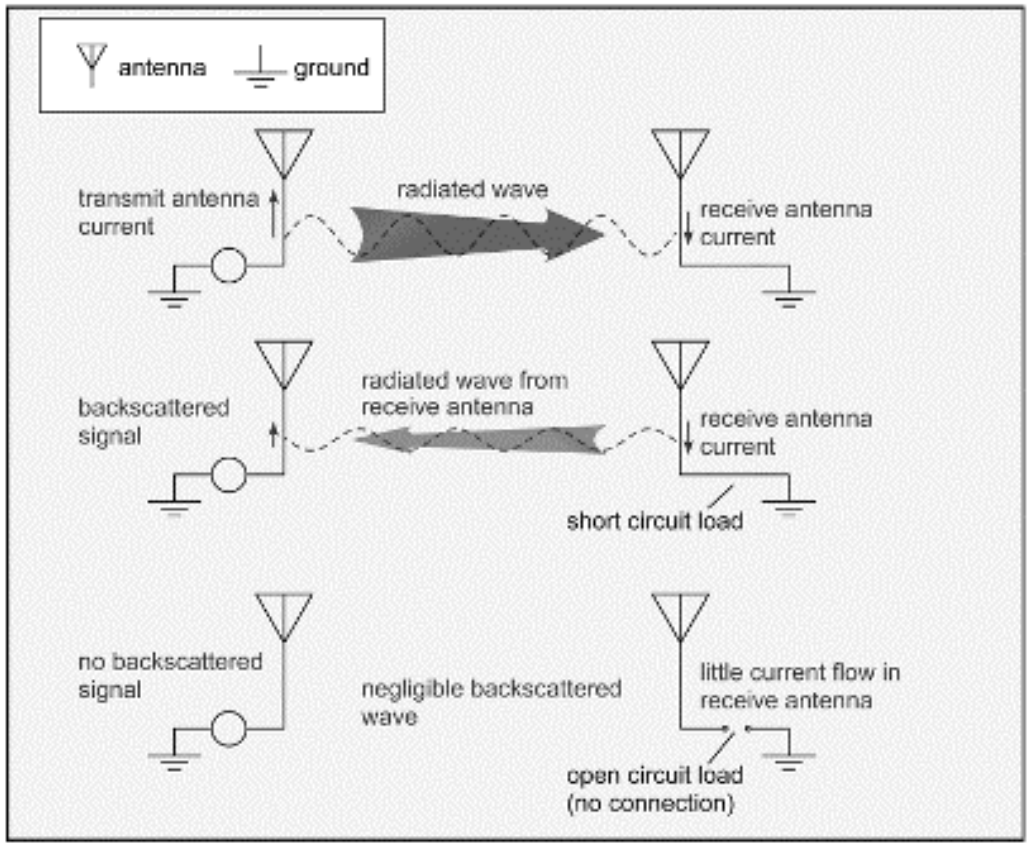
Tag-to-reader Communication



Source: Dan Dobkin "Quick Introduction to RFID", http://www.polygait.calpoly.edu/tutorial.htm

Backscattering

- **Stromversorgung durch Continuous Wave (CW) vom Lesegerät**
- **Tag kodiert seine Antwortet durch die Veränderung seiner Antennen-Impedanz**



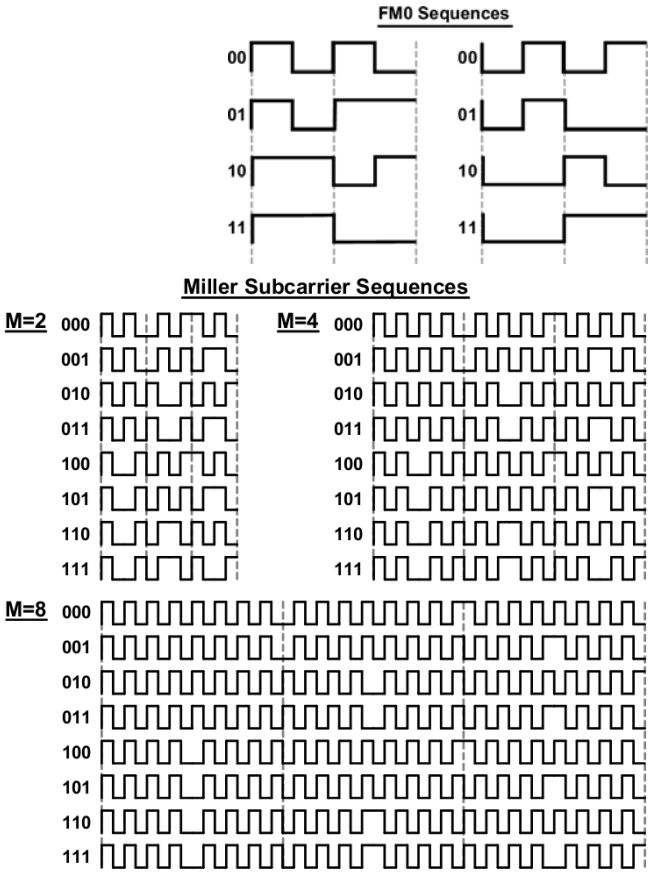
Quelle: Daniel M. Dobkin, "The RF in RFID – UHF RFID in Practice"

EPC Class 1 Generation 2 Uplink Encoding

- *Tag Antworten:*

Pilot Tone	Präambel	Nachricht	End-of-Signaling

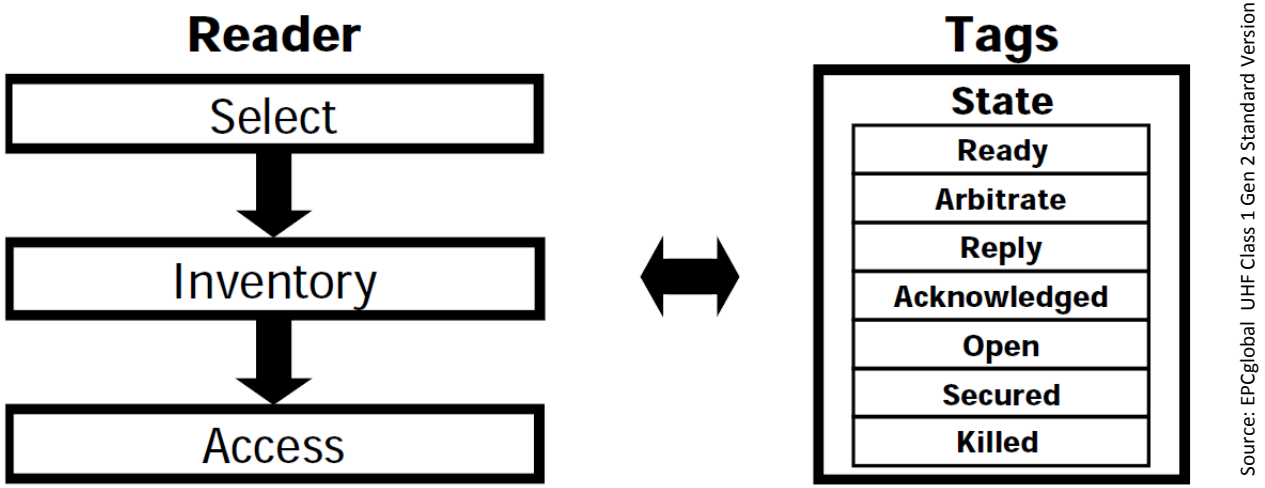
- *Encoding:*
  - *FM0*
    - Phasenwechsel in data-0 Symbol
    - Phasenwechsel nach jedem Symbol
  - *Miller 2/4/8*
    - Phasenwechsel in data-1 Symbol
    - Phasenwechsel nach aufeinanderfolgenden data-0 Symbolen
    - Rechteckkurve mit M-facher Symbolrate multiplikativ verknüpft



Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2

Geschwindigkeit vs. Robustheit

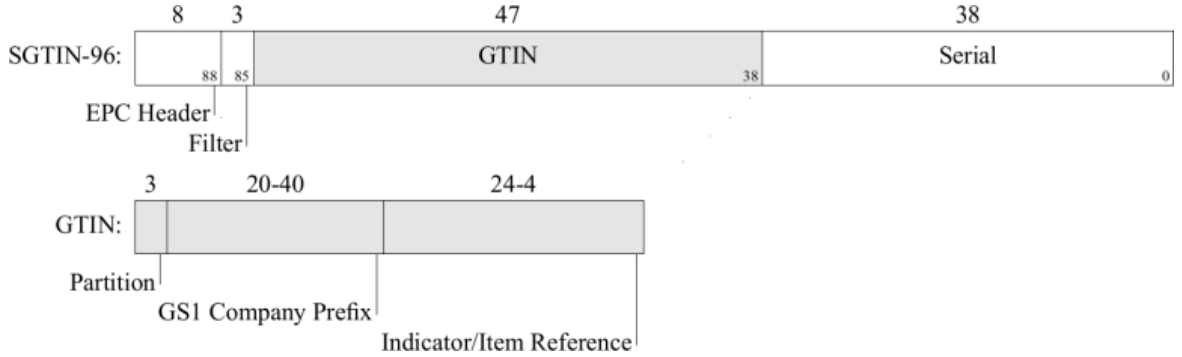
RFID Medium Access – Managing Tag Populations



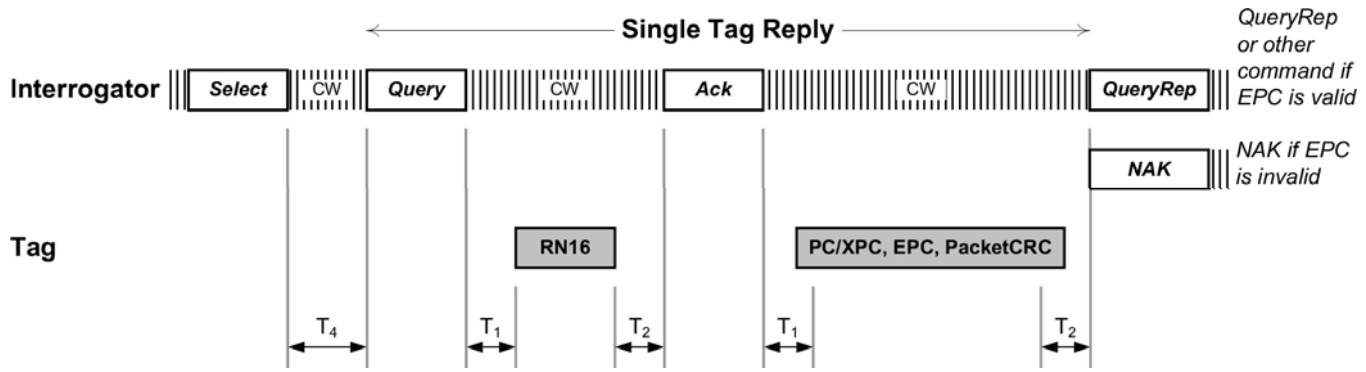
Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2

- **Select**: Interrogator **selects a Tag population** for subsequent inventory
- **Inventory**: Interrogator **identifies Tags** (detect EPC)
- **Access**: Interrogator **transacts with an individual Tag**.
  - reads, writes, authenticates, …

- **EPC – Electronic Product Code:**



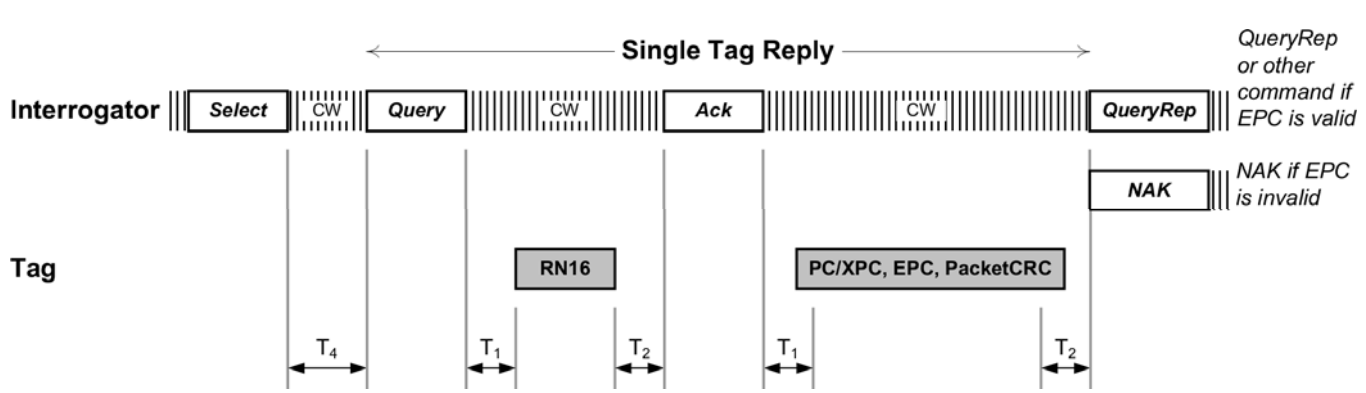
RFID Medium Access – Managing Tag Populations (2)



Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2

- **Select**: Interrogator **selects a Tag population** for subsequent inventory
  - selection is based on **user-defined criteria** (based on flags)
    - enabling union (U),
    - intersection (∩), and
    - negation (~)
  - when (not-killed) Tag receives a **select**
    - returns to the ready state (“holding state” for energized Tags)
    - evaluates the criteria
    - modifies its SL or inventoried flag

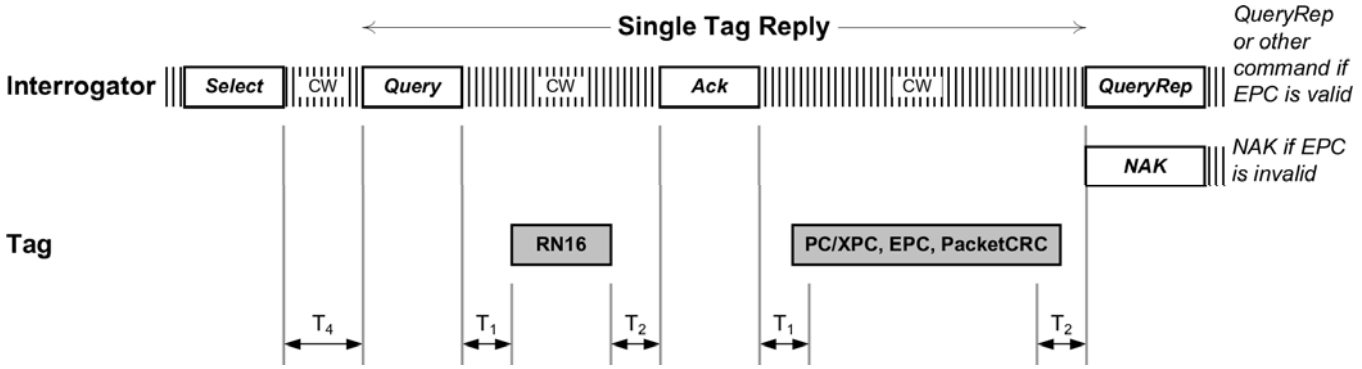
RFID Medium Access – Managing Tag Populations (3)



Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2

- **Inventory:** Interrogator **identifies Tags** (detect EPC)
  - **Query**
    - contains a **slot-count parameter Q** in [0:15] (typically 4) and a **session** parameter (S0 .. S3)
    - Tags pick a random value in the range [0:2^{Q}-1]
      - 0 => reply immediately
      - !0 => transition to the ***arbitrate state*** and await a QueryAdjust /QueryRep command
  - **ACK** (reply the same RN16)
  - **QueryRep** (or QueryAdjust with new Q),
    - to make Tag change its flags (e.g., inventoried flag)
    - causing another Tag to initiate a query response dialog
    - repeat **session** parameter
  - **NAK**
    - all Tags in the inventory round that receive the NAK return to ***arbitrate*** without changing their inventoried flag

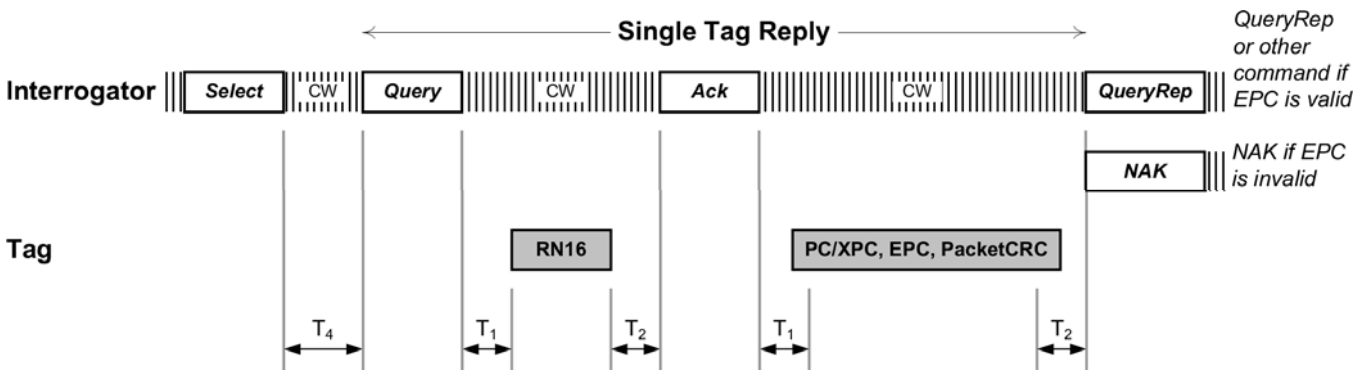
RFID Medium Access – Managing Tag Populations (4)



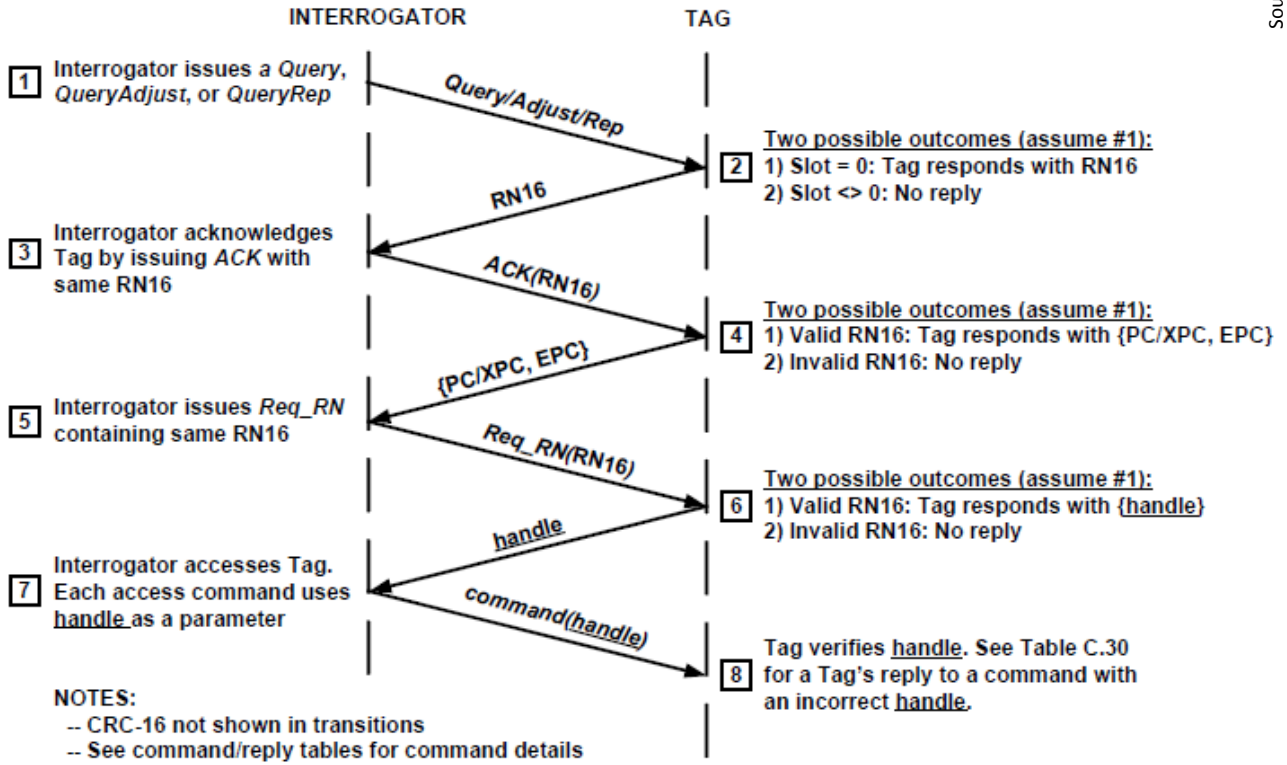
Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2

- **Access:** Interrogator **transacts with an individual TagQuery**
  - an Interrogator may choose to access a Tag after acknowledging it
  - **Req_RN** to acknowledge Tag -> Tags replies with **new RN16** (handle)
    - all following access commands include a Tag's handle
    - handle value is fixed for the entire duration of a Tag access
  - **Read** read Tag memory
  - **Write** write Tag memory
  - **Lock** configure portions of Tag memory to be (un)changeably
  - **Kill** kill a Tag -> once killed, a Tag shall not respond to an Interrogator thereafter
  - **Access** transition a Tag from the open to the secured state
  - …

RFID Medium Access – Managing Tag Populations (5)

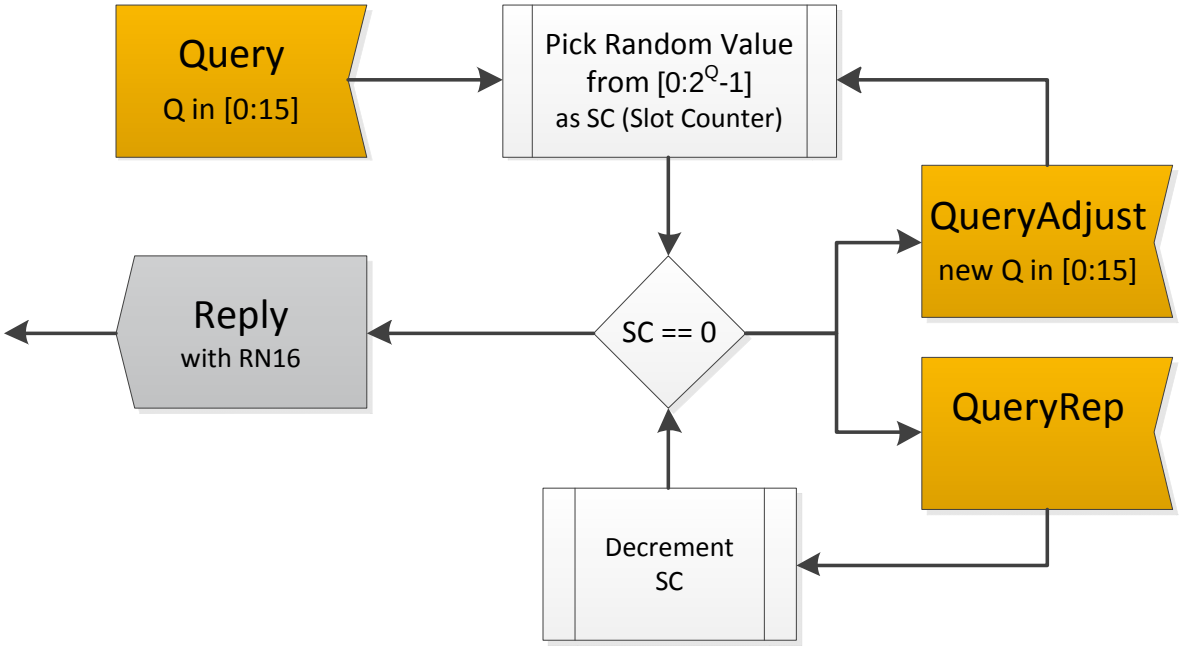


Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2



Source: EPCglobal UHF Class 1 Gen 2 Standard Version 2

RFID Medium Access – Q-Algorithm



Tag-response probabilities range from: $2^0 = 1$ to $2^{-15} = 0.000031$

Is it **polling** or is it **random access**?

- **Frame Slotted Aloha (FSA)**
- **Q Algorithm / Q Protocol** -> dynamic adjustment of Q

aktuelle Informatik-Forschungsfragen im Bereich RFID – Klassifikation

1) Effiziente Datensammlung
   - Wie kann man Tags effizient erfassen? (Durchsatz steigern, ..)
   - Kollisionsvermeidung (1:n) – ein Reader liest viele Tags.
   - Kollisionsvermeidung (m:n) – mehrere Reader lesen viele Tags.
2) Optimierung für Anwendungen
   - Abschätzung der Kardinalität (Anzahl Tags)
   - Missing-Tag-Identification
   - Lokalisierung mittels RFID
3) Sicherheit
   - Verschlüsselung
   - Architekturen
4) Integration von Sensordaten
   - Sensor-Tags
   - Optimierungen fürs Auslesen von Sensordaten
   - MAC-Protokolle
5) Kombination von RFID und WSN