Wireless Networking [ET4394]

Radio Frequency Identification (RFID)

Przemysław Pawełczak

Amjad Y. Majid

TU Delft

Learning objectives (LOs)

- **LO1:** To understand the operating principles of RFID
- **LO2:** To understand EPC Class 1 Gen 2 protocol
- **LO3:** To gain knowledge about the WISP 5 platform

Outline

- RFID / CRFID
- EPC1 Gen2
  - Reader to Tag
    - Messages sequence
    - A message details (An example)
  - Tag to Reader
    - Backscattered signal

Literature

- Joshua R. Smith et al., **Wirelessly Powered Sensor Networks and Computational RFID**, Springer, 2013
  - www.springer.com/gp/book/9781441961655
- K. Finkenzeller, D. Muller, **RFID Handbook**, Wiley, 2010
  - rfid-handbook.de/the-book/english-edition.html
- **EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID v2.0.0**, EPCGlobal, 2013
  - http://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf

RFID: Introduction

- **Radio Frequency Identification**: wireless communication technology used to identify/track
- **RFID** is everywhere (NFC, Products inventory, Credit card, OV card)

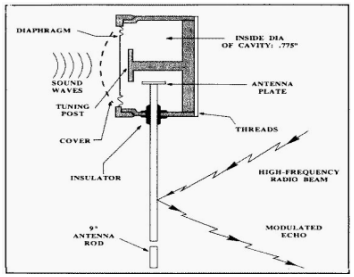
www.sparkglobaltech.com
www.haagsetijden.nl
http://www.nowtheendbegins.com/
www.computerworld.com

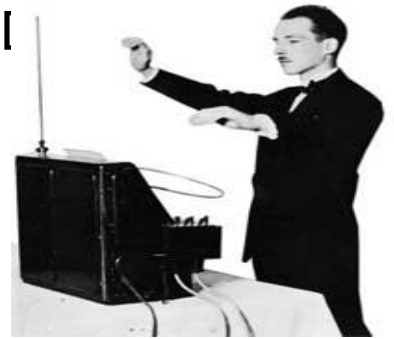
History of RFID

- **WW II** "Friend or Foe" identification systems (Radar)
- **1946** Lev Sergeyevich Termen: "The Thing"
- **1948** H. Stockman, *Communication by Means of Reflected Power*, Proceedings of the IRE, Oct. 1948
- **1970s** First RFID patents: New York Port Authority demonstration
- **1998** First RFID passports
- **2004** EPC Class 1 Gen 2 protocol
- **2008** First Intel WISP released

"RFID" in the Cold War

- The Thing
  - "Gift" from **Russia** to **US Embassy** in 1946
  - Listening device
  - Invented by **Léon Theremin** (also: youtu.be/w5qf9O6c20o)
  - Uses **Backscatter Communication** like RFII
  - Undiscovered until 1952





Source: http://electrocompost.blogspot.nl/2010/11/instrumentos-curiosos-theremin.html
http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/mil/cavity/index.html

Types of RFID (cont.)

- **Class 1**
  - Passive, read-only
  - Backscatter
  - One-time field-programmable non-volatile memory
  - EPC Gen2 compliant
- **Class 2**
  - Same as Class 1
  - Up to 65 KB read-write memory
- **Class 3**
  - Same as class 2, but with built-in battery to extend read range.
- **Class 4**
  - Active
  - Transmit signals to readers
- **Class 5**
  - Active
  - Can communicate with other Class 5 devices and/or other devices

Types of RFID

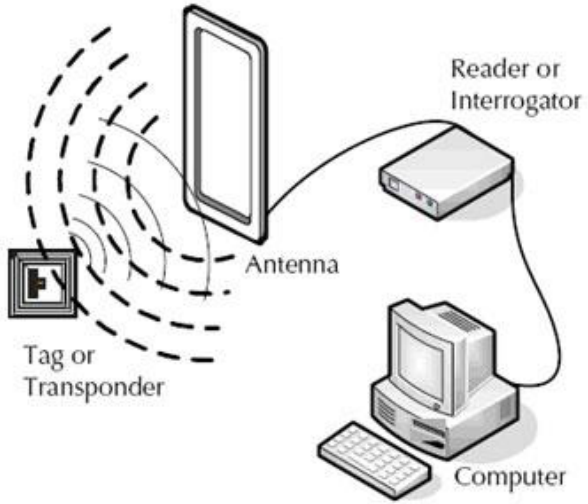
- **Active**
  - Battery operated
  - Low signal strength needed for communication
  - High cost per tag
  - Low infrastructure cost
  - High range
- **Passive**
  - No internal power source
  - Harvest energy from reader antenna
  - Low cost per tag
  - High infrastructure cost (reader)
  - Low range

Frequency Ranges

- **Low Frequency** (125-134 kHz)
  - Used for animal identifications
  - Up to **10 cm** range
- **High Frequency** (13.56 MHz)
  - Used for NFC, smart cards, tickets and DVD kiosks
  - Up to **30 cm** range
- **Ultra-High Frequency** (433 MHz and 856-960 MHz)
  - Used in all types of applications
  - Up to **12 m** range (passive, tag dependent)
  - FCC (US standard, 902-928 MHz) and ETSI (EU standard, 865-868 MHz)
- **Microwave** (2.45 GHz)
  - Used for Electronic toll collection, goods tracking and production line tracking
  - Up to **2 m** range (passive)

RFID: System Overview

- Antenna
- IC
- Tiny memory
- Energy Harvester



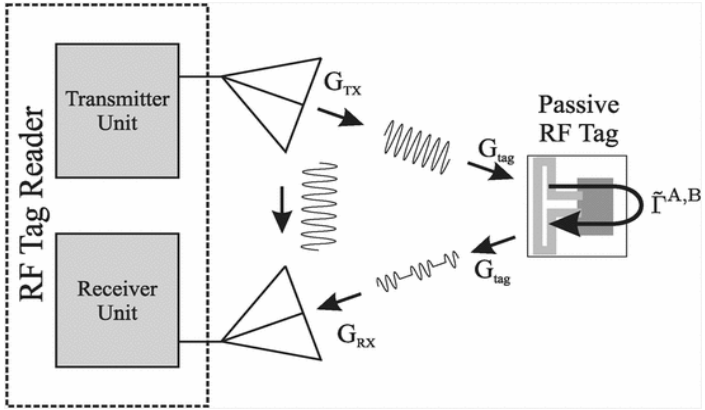
RFID system overview

https://www.barcodesinc.com/

http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=4447347

Modulation

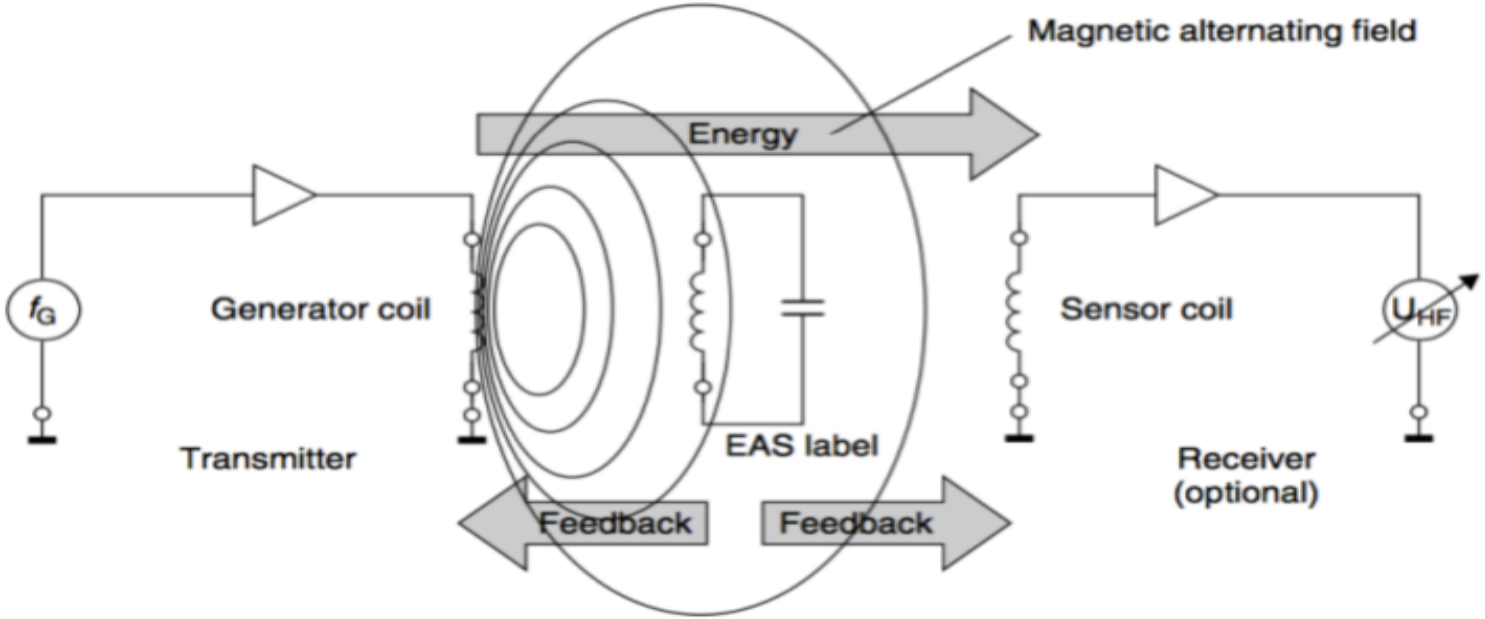
- **Backscatter (UHF)**
  - Reader emits wave
  - Upon receiving, the RF tag reflects the wave to modulate



http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=4447347

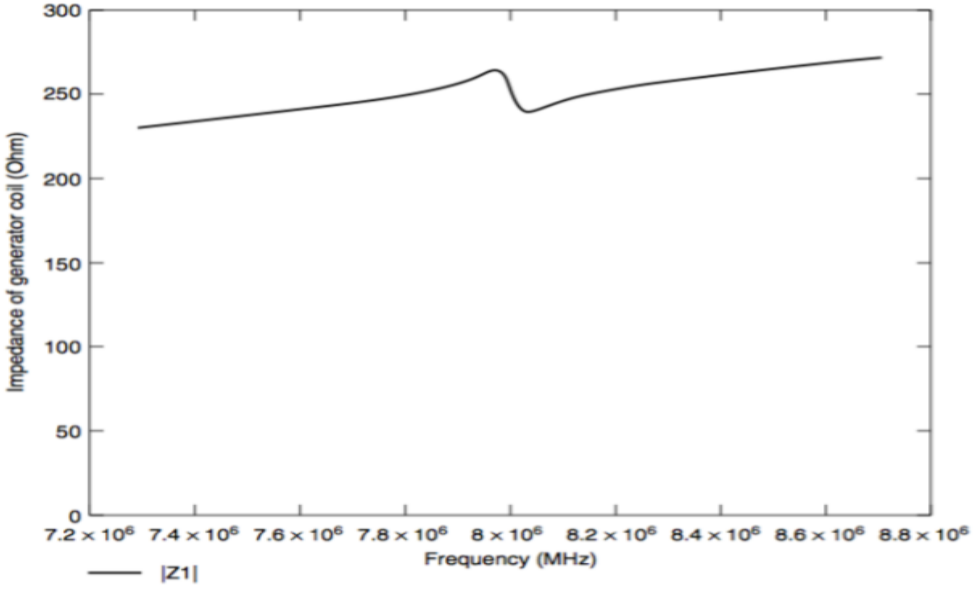
The Basics:

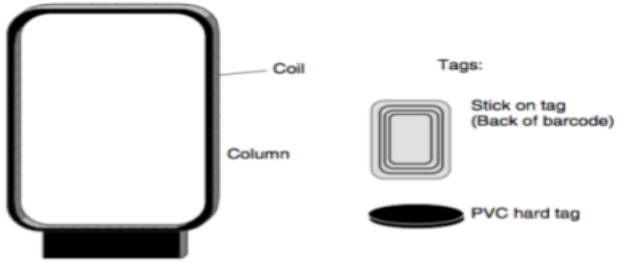
Electronic Article Surveillance



Source: K. Finkenzeller, **RFID Handbook**, Wiley, 2010

Electronic Article Surveillance (cont.)

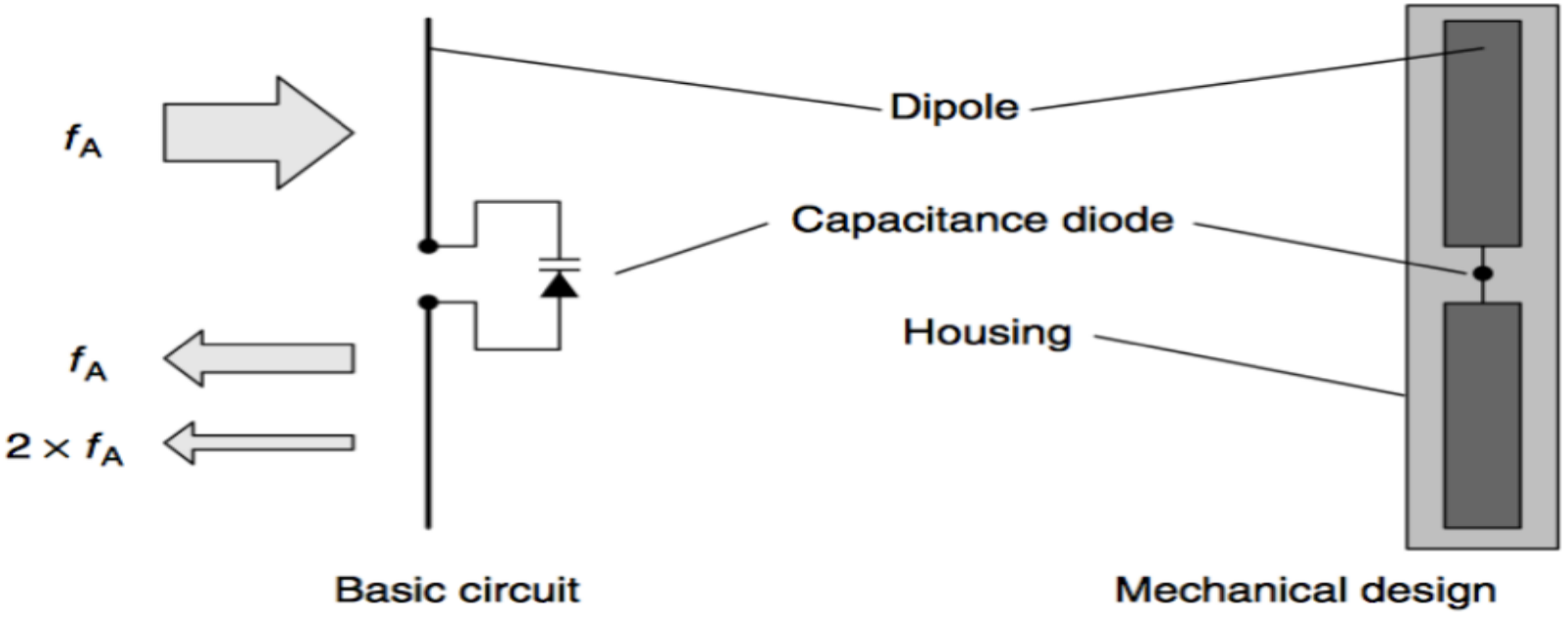




Source: K. Finkenzeller, **RFID Handbook**, Wiley, 2003

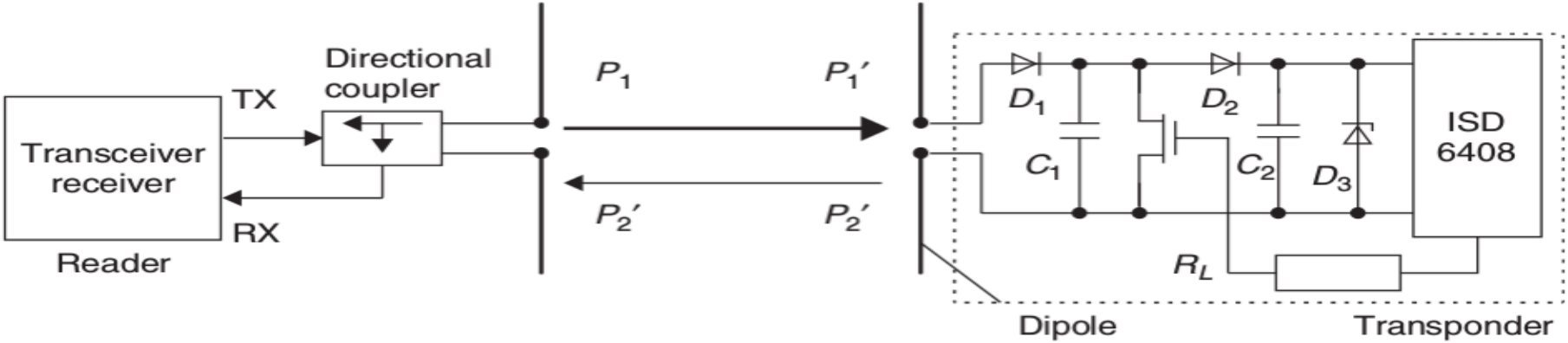
Source: K. Finkenzeller, **RFID Handbook**, Wiley, 2010

Electronic Article Surveillance (cont.)



Source: K. Finkenzeller, **RFID Handbook**, Wiley, 2010

More Advanced:
Backscatter Radio



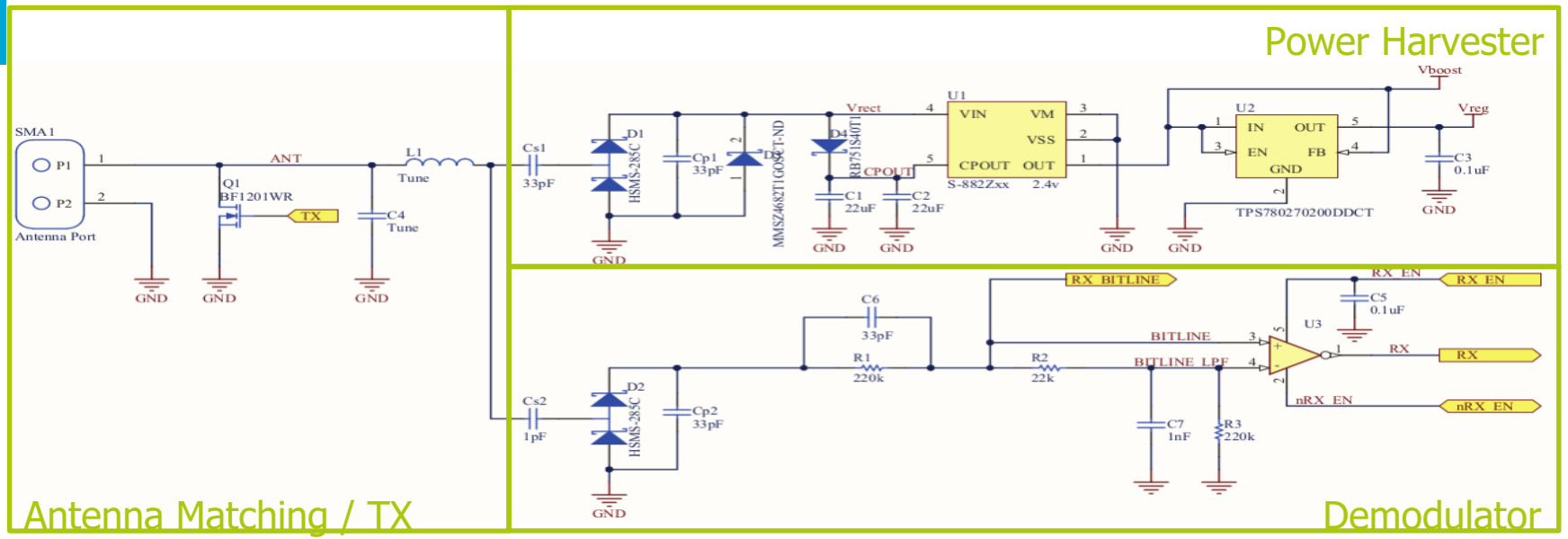
ISD6408: UHF Code Generator

Source: K. Finkenzeller, **RFID Handbook**, Wiley, 2010

Wireless Sensing and Identification Platform (WISP)

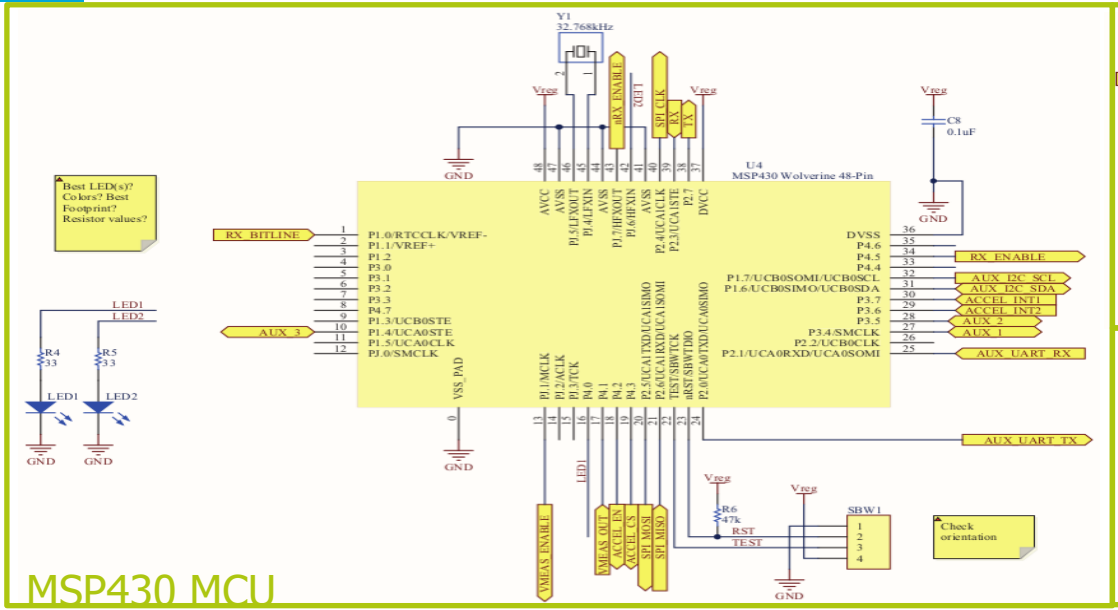
- Class 2 tag with onboard MCU and memory
- Computational RFID Device
- First founded at Intel Labs, Seattle
- Now maintained by University of Washington, Seattle
- Opened new research topics and challenges
- MSP430FR5969 with FRAM on WISP5

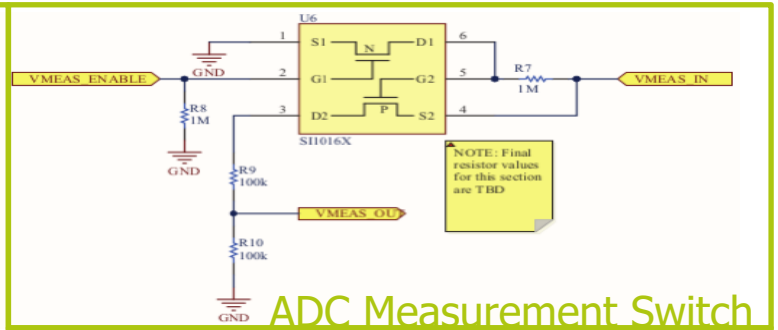
WISP Hardware Excerpt

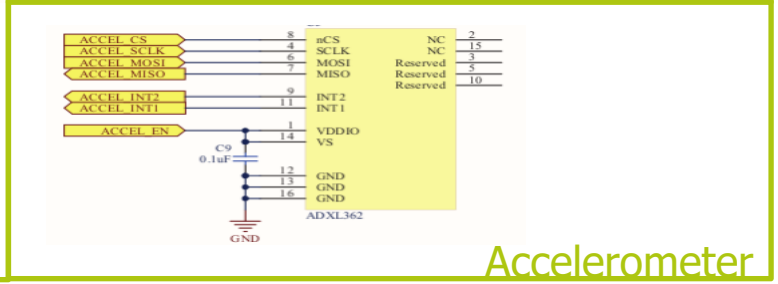


http://wisp5.wikispaces.com/WISP+Hardware

WISP Hardware Excerpt (cont.)

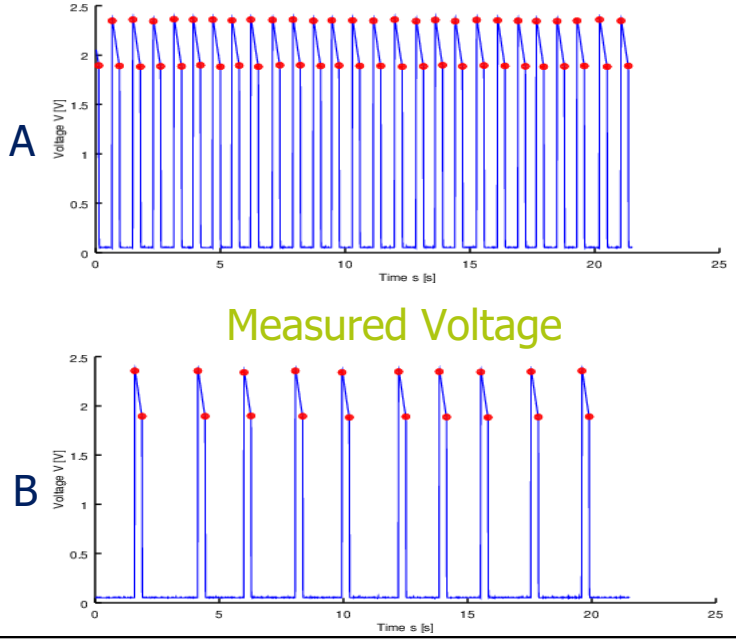




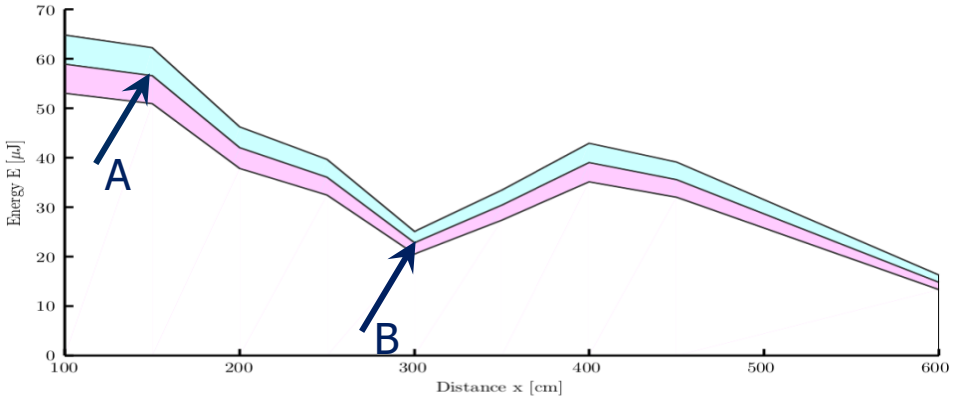


http://wisp5.wikispaces.com/WISP+Hardware

WISP Performance Harvester



Measured Voltage



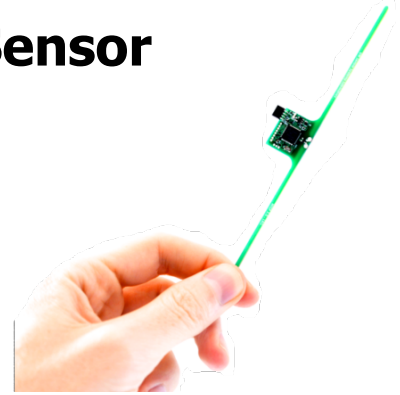
Calculated Energy

Note: Energy +/-10% because of capacitor accuracy

WISP @ TU Delft

- We are the **LARGEST** research group outside the USA!
- **Robust Downstream Communication on Transient Powered Computational RFID Devices**, J. Tan

- **BLISP: A Hybrid Ultra Low Energy Wireless Sensor Node for <application TBD>**, I.J.G. in 't Veen
- **<Some open project>**
  - Interested in graduation project?
  - Send mail to p.pawelczak@tudelft.nl or drop by at EWI HB 09.050



EPCglobal Class 1 Generation 2

EPC

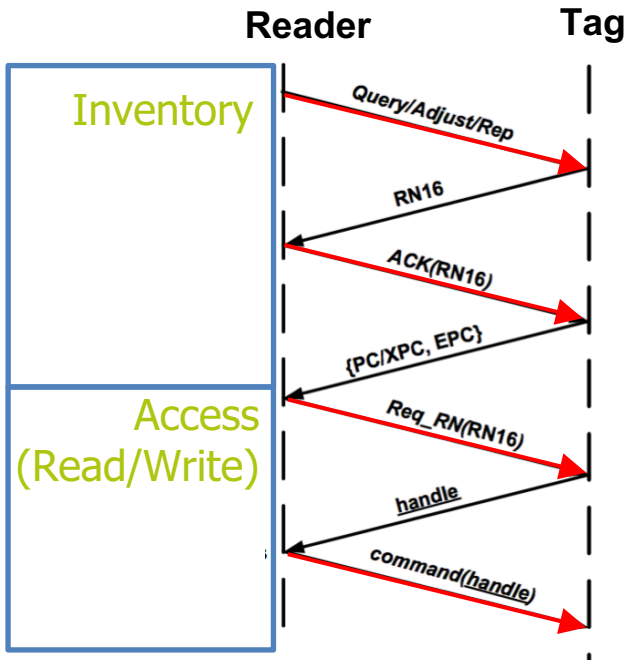
- ISO 18000-6C
- Specially for passive UHF backscatter RF tags
- Features
  - Reader talk first
  - Tags can be read, written, and killed in the field
  - A killed tag does nothing and remains killed forever
  - Flexible data rates
  - Provides methods for spectral control to avoid interference
  - Uses a Slotted-Aloha algorithm to mitigate data collisions

Source: **EPC Protocols Gen2 UHF RFID v2.0.0**, EPCGlobal, nov 2013

Source: **The Fundamentals of Backscatter Radio and RFID Systems**, Disney Research Pittsburg, 2009

Reader to Tag Messages

EPC C1 Gen2 (R=>T)

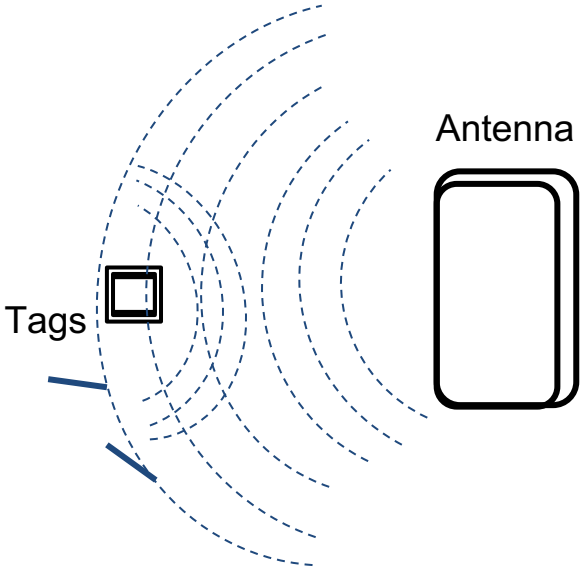


- **Query:** starts an inventory round
- **QueryRep:** indicates the beginning of a slot
- **QueryAdjust**: adjusts the number of slots
- **Command**: Can be Read, Write, BlockWrite

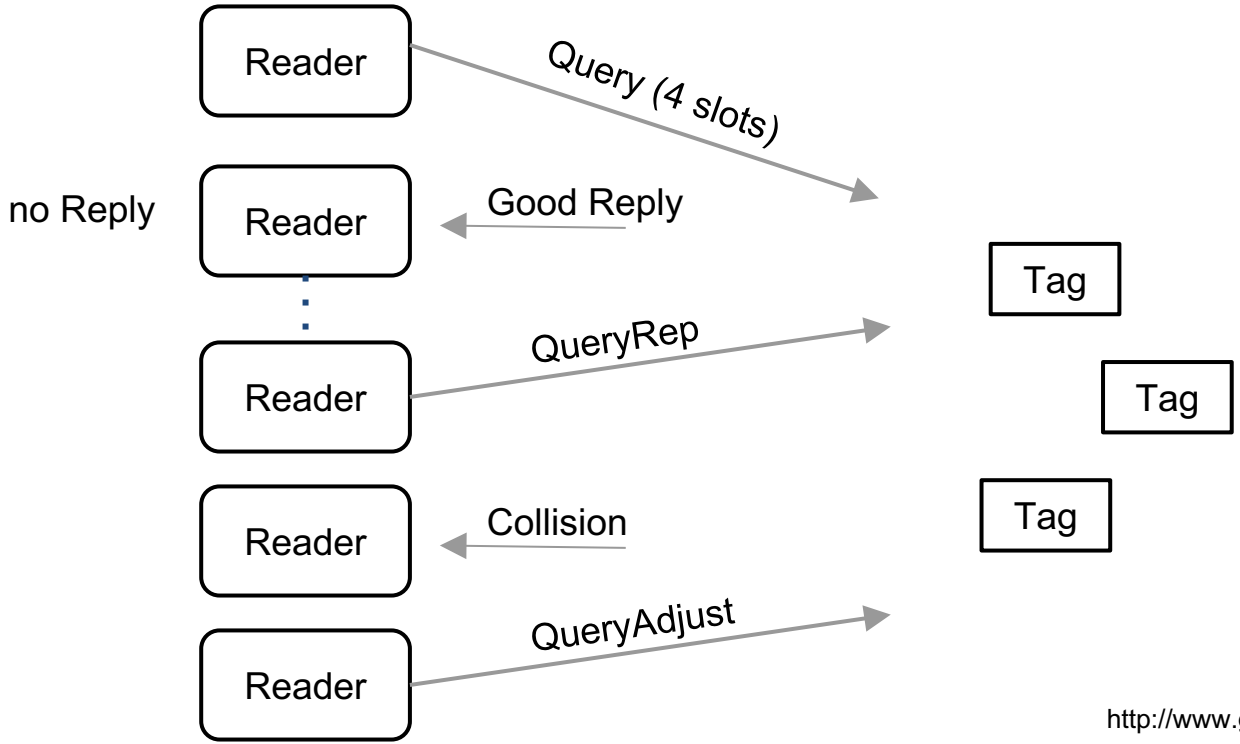
http://www.gs1.org/

EPC C1 Gen2 Overview

- EPC **goal** is to enable the **reader** to **identify** all tags
- Collisions may occur
- Slotted Aloha
  - Within a slot only one tag should reply



EPC (R=>T) Inventory



http://www.gs1.org/

Messages Preambles

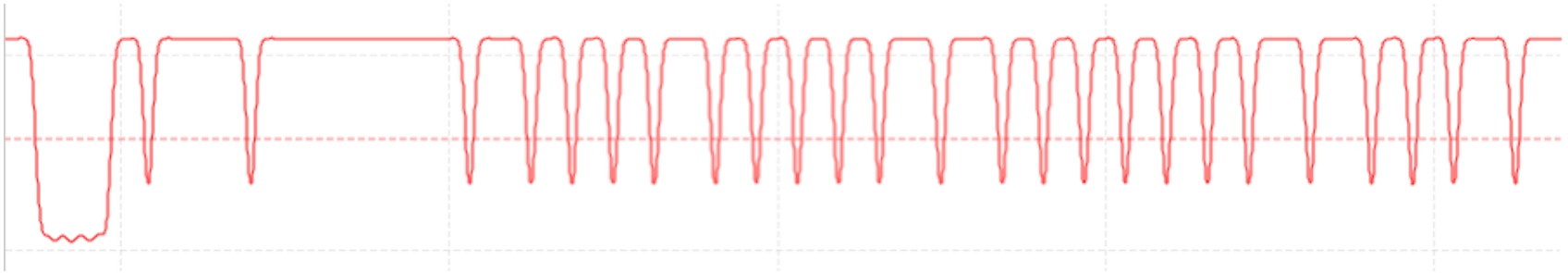
Command	Code	Length (bits)
QueryRep	**0**0	4
ACK	**0**1	18
Query	**1**000	22
QueryAdjust	**1**001	9
Select	**1**010	> 44
Reserved for future use	**1**011	–
NAK	**11**000000	8
Req_RN	**11**000001	40
Read	**11**000010	> 57
Write	**11**000011	> 58

http://www.gs1.org/

Query Message

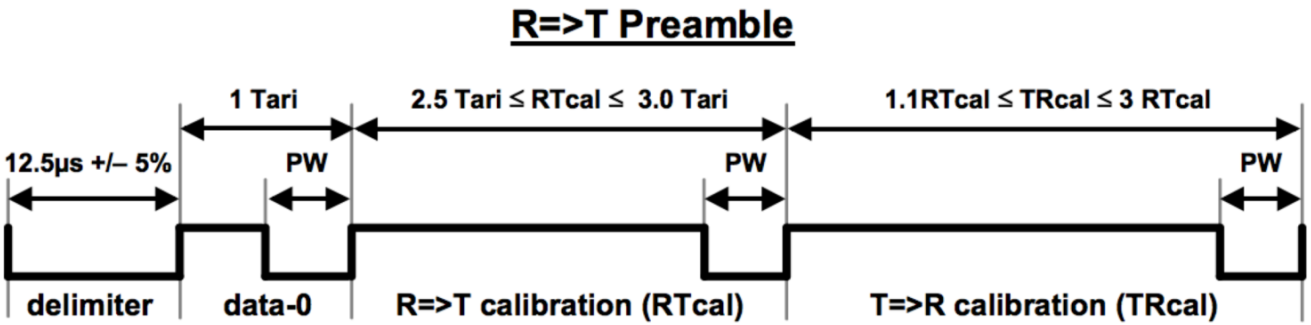
Table 6.32: *Query* command

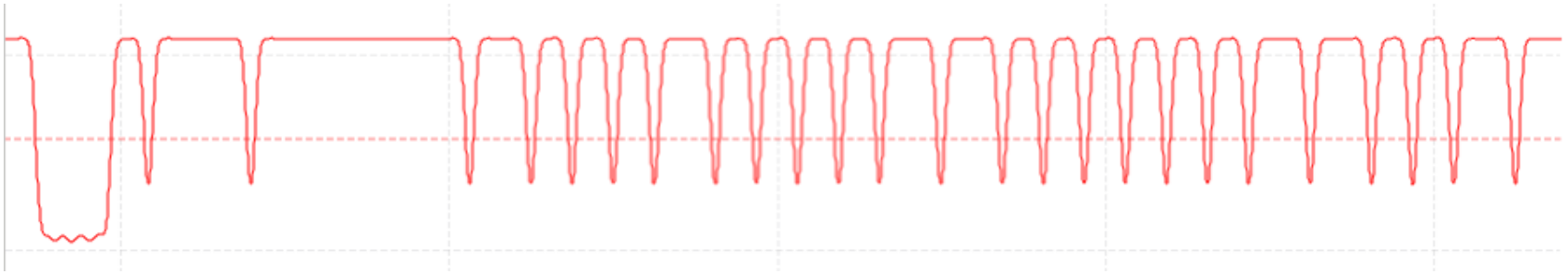
	Command	DR	M	TRext	Sel	Session	Target	Q	CRC
# of bits	4	1	2	1	2	2	1	4	5
description	1000	0: DR=8 1: DR=64/3	00: M=1 01: M=2 10: M=4 11: M=8	0: No pilot tone 1: Use pilot tone	00: All 01: All 10: ~**SL** 11: **SL**	00: S0 01: S1 10: S2 11: S3	0: *A* 1: *B*	0–15	CRC-5



http://www.gs1.org/

Message Preamble





http://www.gs1.org/

Modulation (Reader signals)

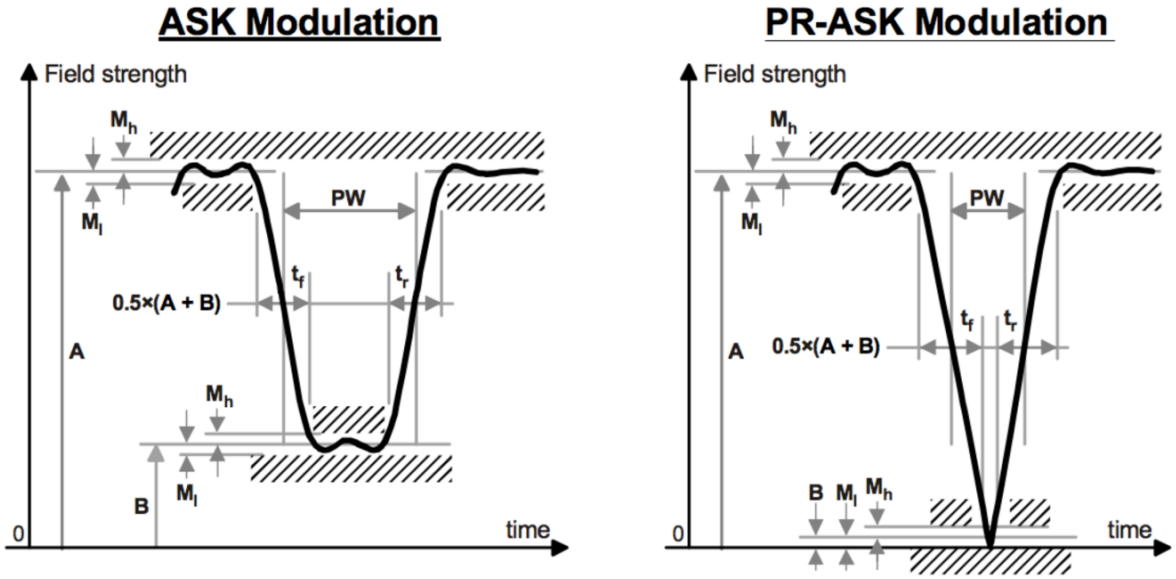


Figure 6.2: Interrogator-to-Tag RF envelope

http://www.gs1.org/

Data Encoding

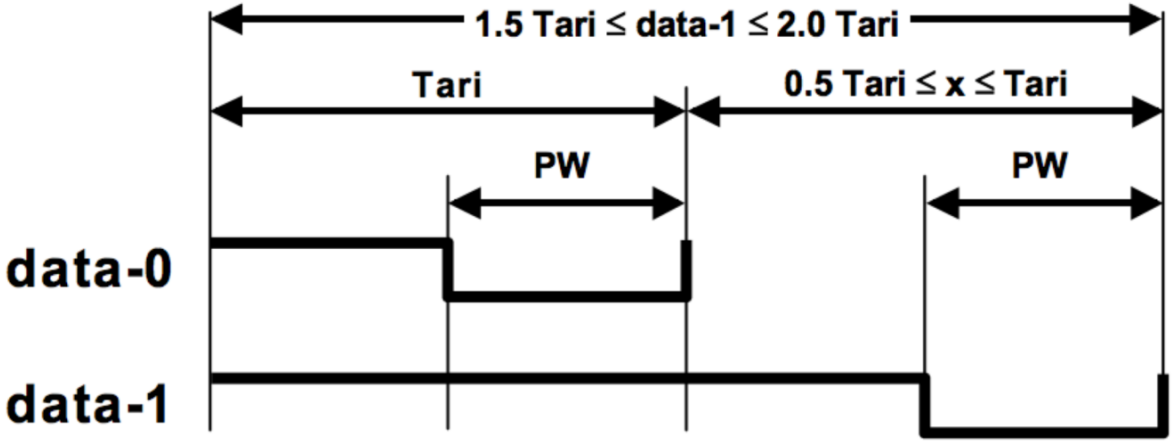
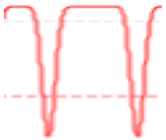


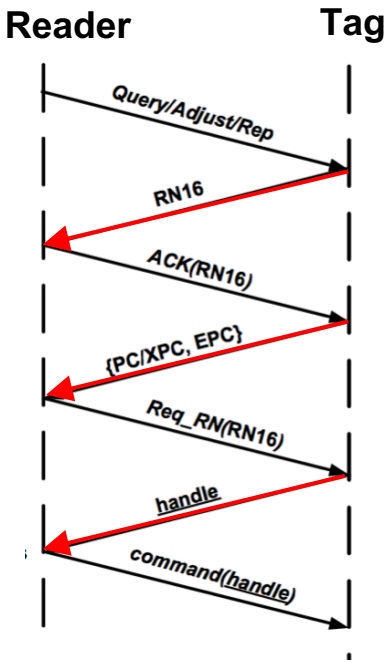
Figure 6.1: PIE symbols



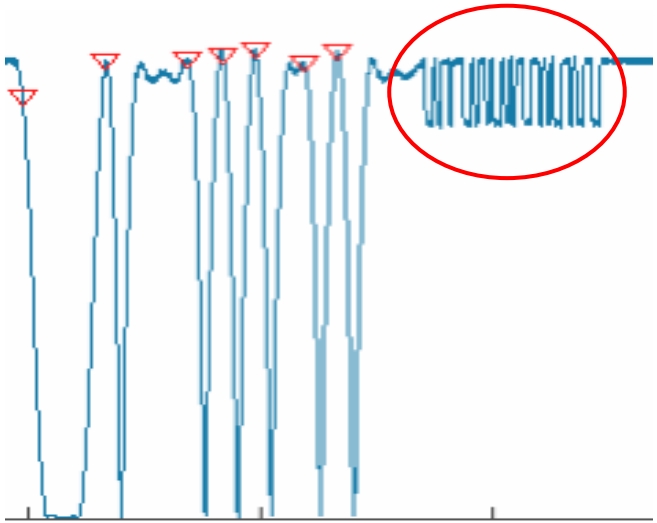
http://www.gs1.org/

Tag to Reader Backscattering

EPC (T=>R) Messages



- **RN16**
- **EPC**
- **handle**



http://www.gs1.org/

Signal Preamble

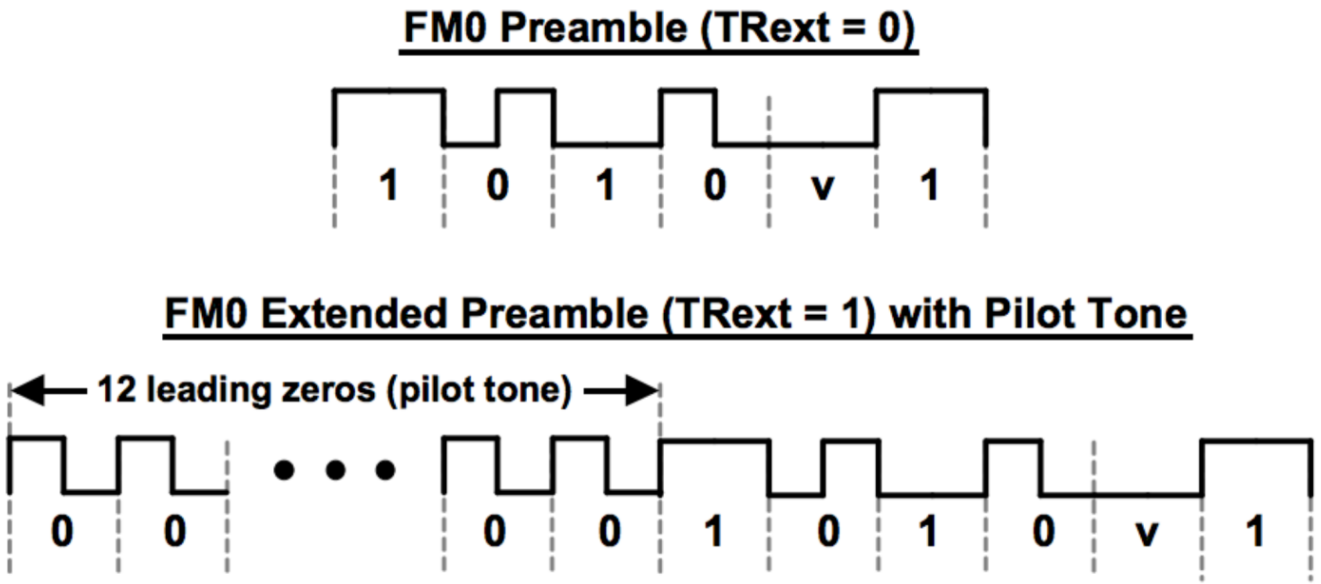


Figure 6.11: FM0 T=>R preamble

http://www.gs1.org/

Data Symbols

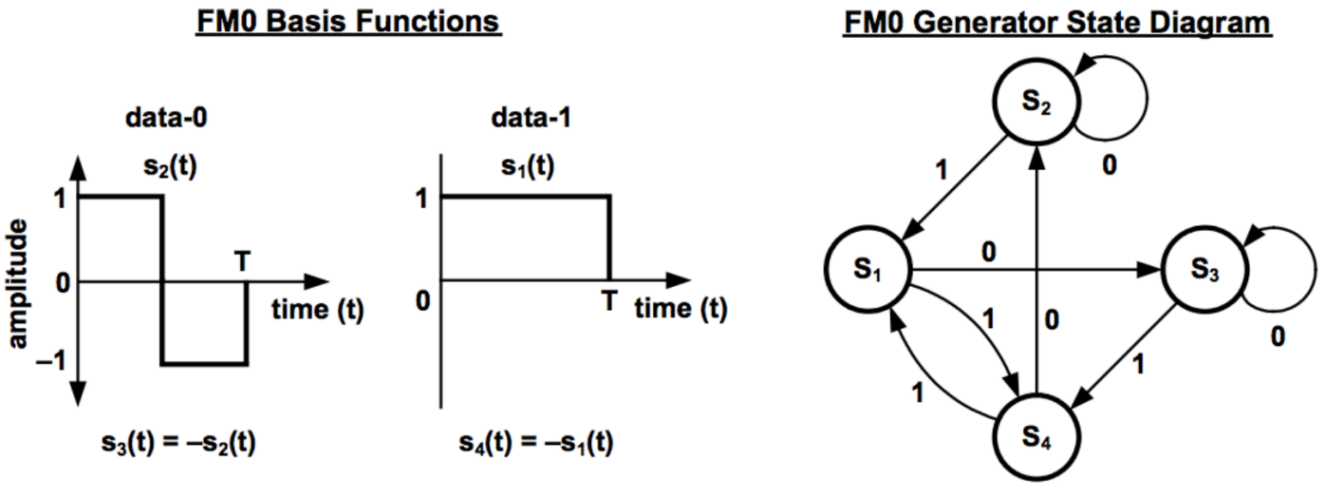
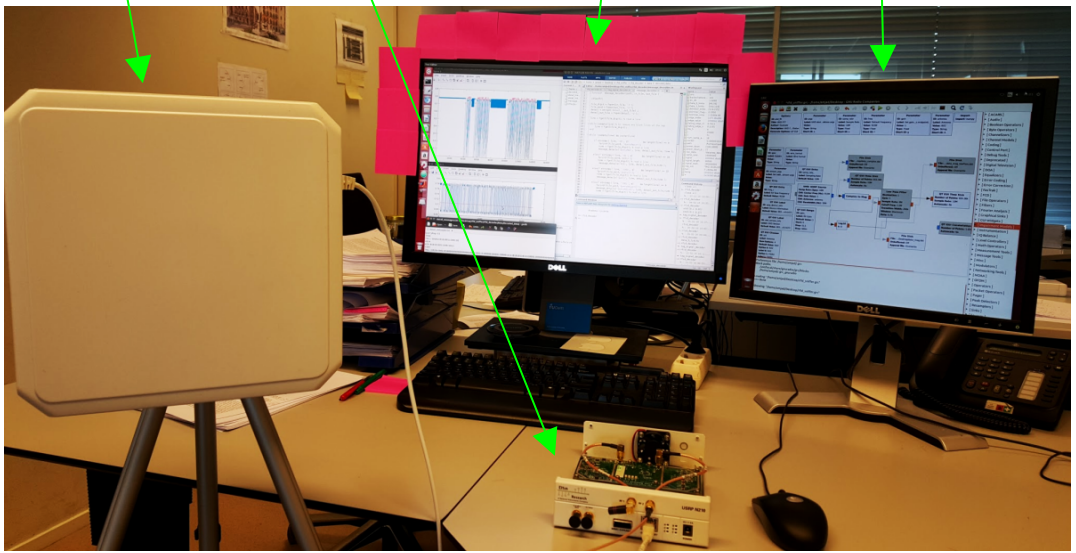


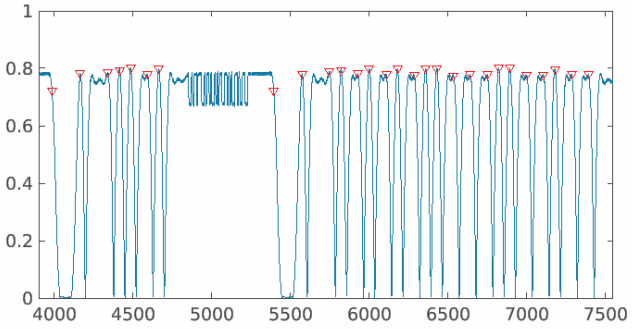
Figure 6.8: FM0 basis functions and generator state diagram

http://www.gs1.org/

TCP Sniffer



Output

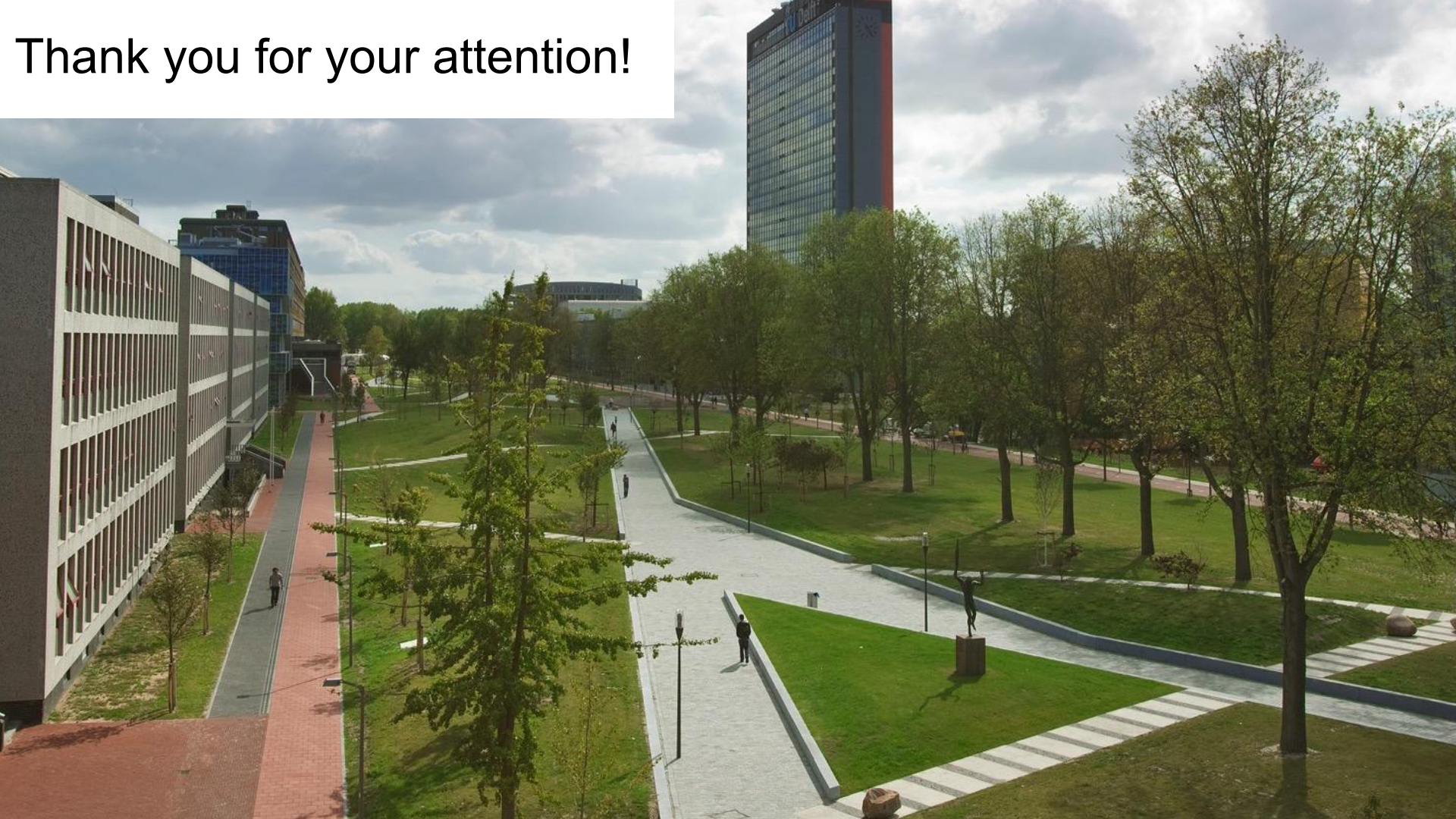


QueryRep:S2 3986

TAG::1010v1010100111001l0 4854

ACK:0101010011100110ll 5394

Thank you for your attention!



EPC C1G2 Anti Collision: Slotted Aloha (Inventory)