

# Zürich University Of Applied Sciences Institute of Embedded Systems InES

## **Microcontroller based passive UHF RFID tags**

**(Presented at Energy Harvesting Conference  
Biel, 27<sup>th</sup> October 2010)**

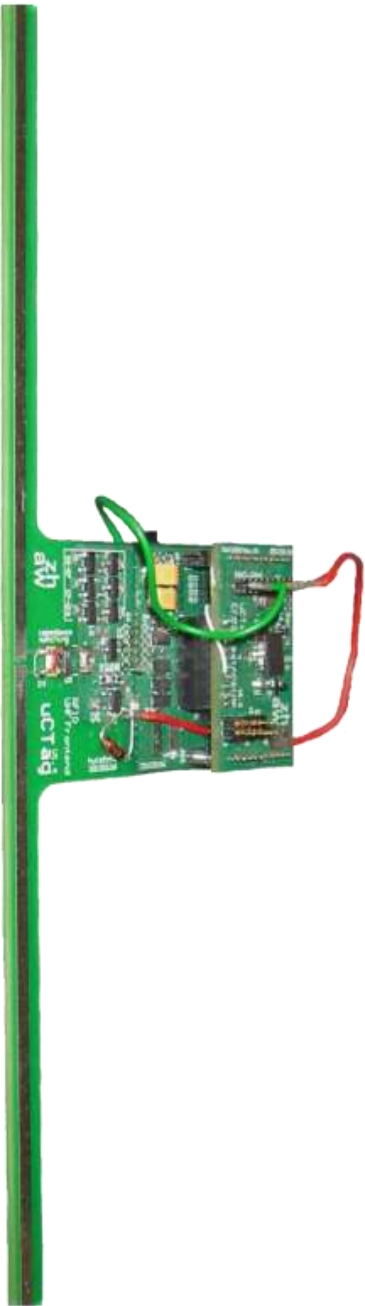
**Dipl. Ing. M. Würth, D.Jäger, Markus Hutzler**

**Prof. Dr. Marcel Meli**

**Contact: [Marcel.Meli@zhaw.ch](mailto:Marcel.Meli@zhaw.ch)**

## Outline

- Who we are (our RFID activities)
- Introduction
- Case for RFID sensors
- The challenges
- $\mu$ cTag
- Implementations
- Tests and results
- Conclusions
- A summary of our wireless/battery-less activities



## Who we are (our activities in RFID).

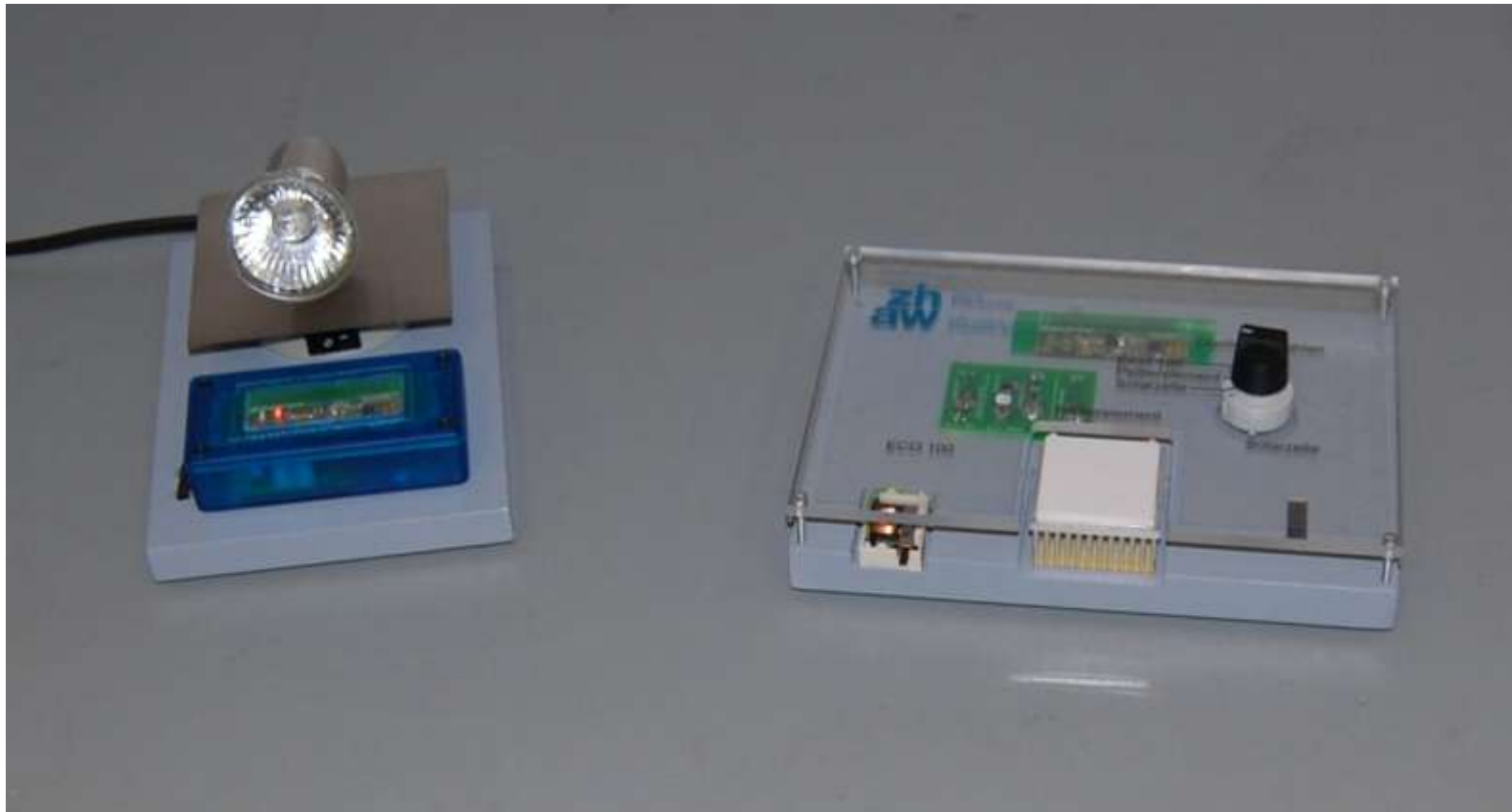
- Institute of Embedded Systems, Winterthur, Switzerland
- Part of Zurich University of Applied Sciences
- Involved in teaching, applied research projects
  - Wired: Industrial Real time communication (Ethernet, ...)
  - Wireless: WPAN, RFID, UWB
  - Energy harvesting, very Low power applications
- Example of radio tag powered with a small solar cell
  - Cheap solar cell (about the third of the area of 1Euro coin)
  - Works in normal office luminosity conditions
  - Several low power microcontrollers (here MSP430)
  - Different wireless protocols (here TI proprietary)
  - “Install and forget”



# Demonstrator: Battery free wireless automation

The receiver controls a lamp

The sender can use different power sources  
EM6819, EM9201, LTC DC/DC for Seebeck

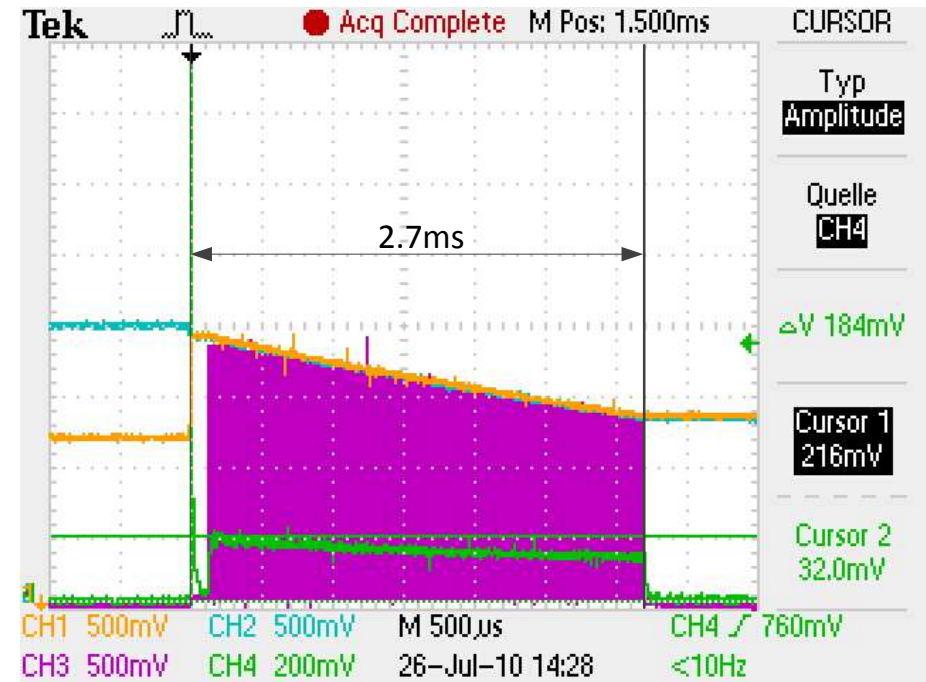
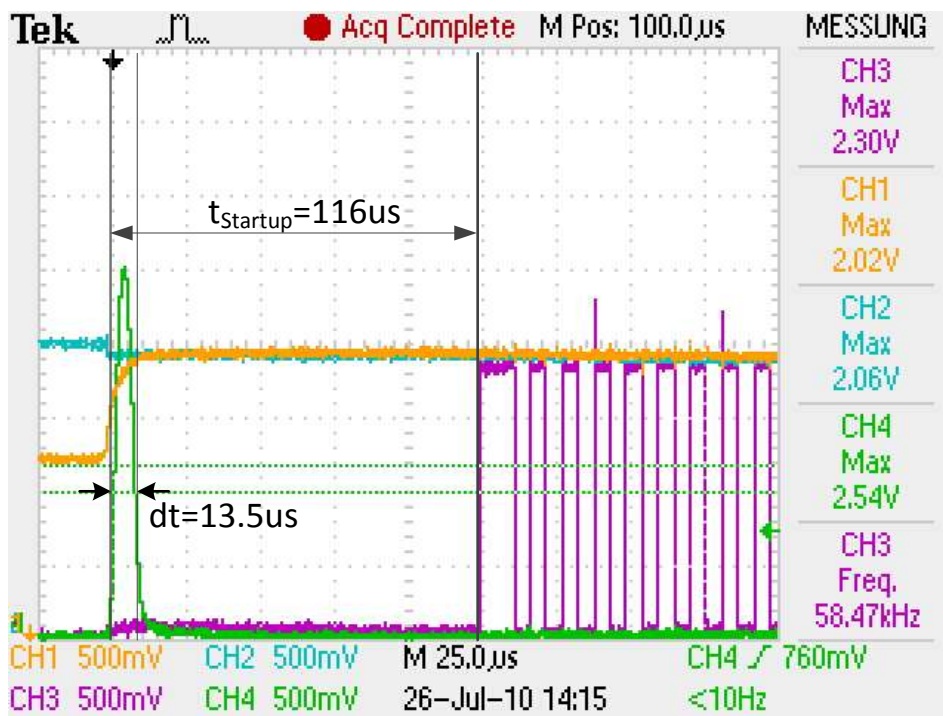


Electro-dynamic Seebeck

Solar



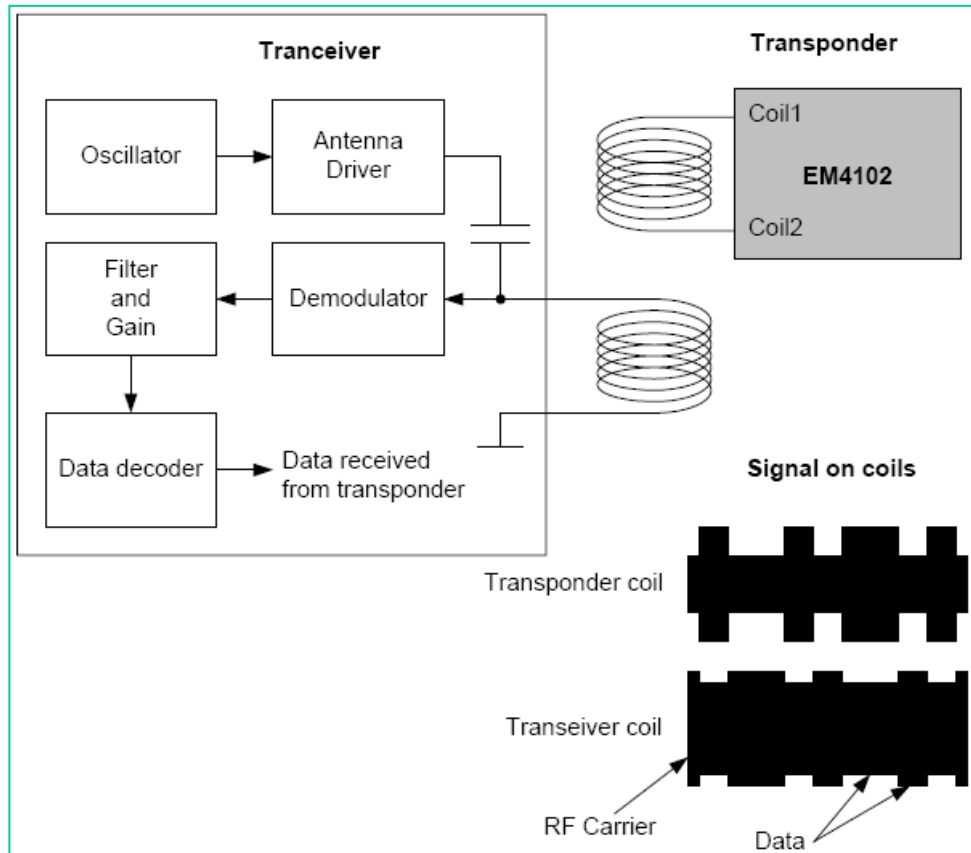
# Start and run a microcontroller on 2 microJ



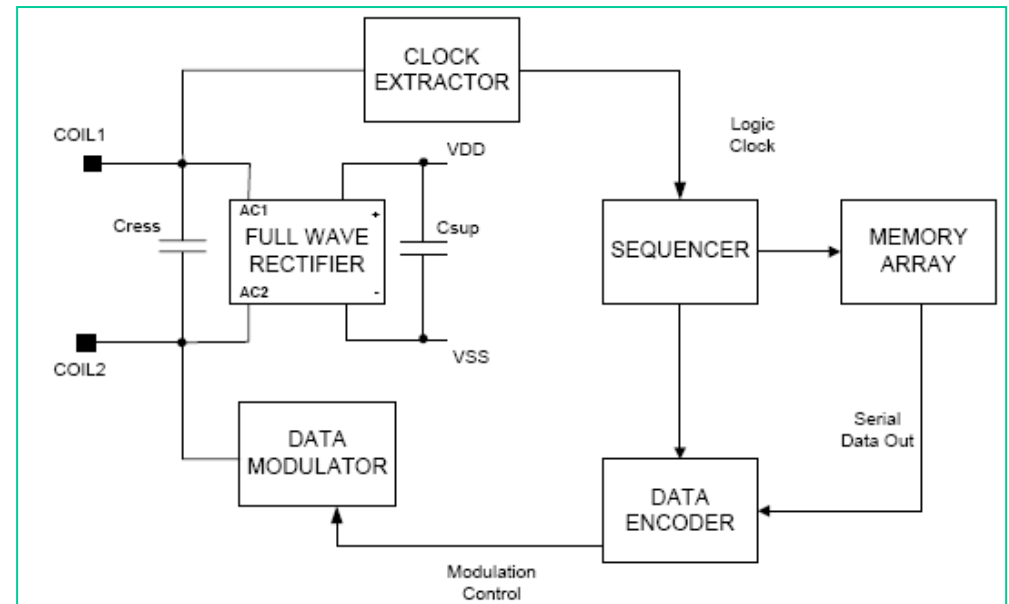
# Introduction

- What are RFID tags
  - Circuits that will wirelessly communicate their identity by using the RF field of a reader
    - Identity is sent to the reader when required
  - Passive tags
    - They draw their energy from the reader
  - Active tags
    - Get all their energy from another source (batteries)
  - Semi-active / Semi-Passive
  - Frequency of operation
    - LF: 125KHz -140 KHz (proximity: magnetic coupling)
    - HF: 13.56 MHz (proximity, vicinity: magnetic coupling)
    - UHD: 868 MHz, 900 MHz (long distance: electromagnetic)
    - 2.4 GHz
  - There are different protocols in use

# Introduction (Example of Tag)



Diagrams taken from datasheet of EM4102 (125KHz tag), EM Marin



## Introduction

- What are RFID sensors?
  - Sensors data is sent in place of identity, or mixed with identity
  - Communicate their measurements to RFID reader .
  - Several readers can be linked together (RSN →RFID Sensor Networks)
    - Temperature/light .... sensors
    - Sensor in the body
- Active (external power source)
  - Sensors sometimes need a lot of energy
- Passive
  - Get their energy from the reader (magnetic/electromagnetic)
    - Need no extra supply
    - Can be used in environment where change of battery is difficult or impossible

## Case for RFID sensors

- Current RFID tags/sensors:
  - Mostly state machines with a sensor
  - Dedicated devices (built for a particular application or sensor)
  - Little/no flexibility in the type of sensor
  - Little/no flexibility in adapting to other protocols
  - There are some intelligent tags, but most use external power sources
    - Based on FPGA/CPLDs ,ARM based micros,...
    - Greedy in energy
  - The WISP is a passive RFID emulation for sensors based on the MSP430 Works down to 1.8 volt
  - $\mu$ Tag developed by InES and first presented at Embedded World 2009 is a passive RFID tag for ID and sensors

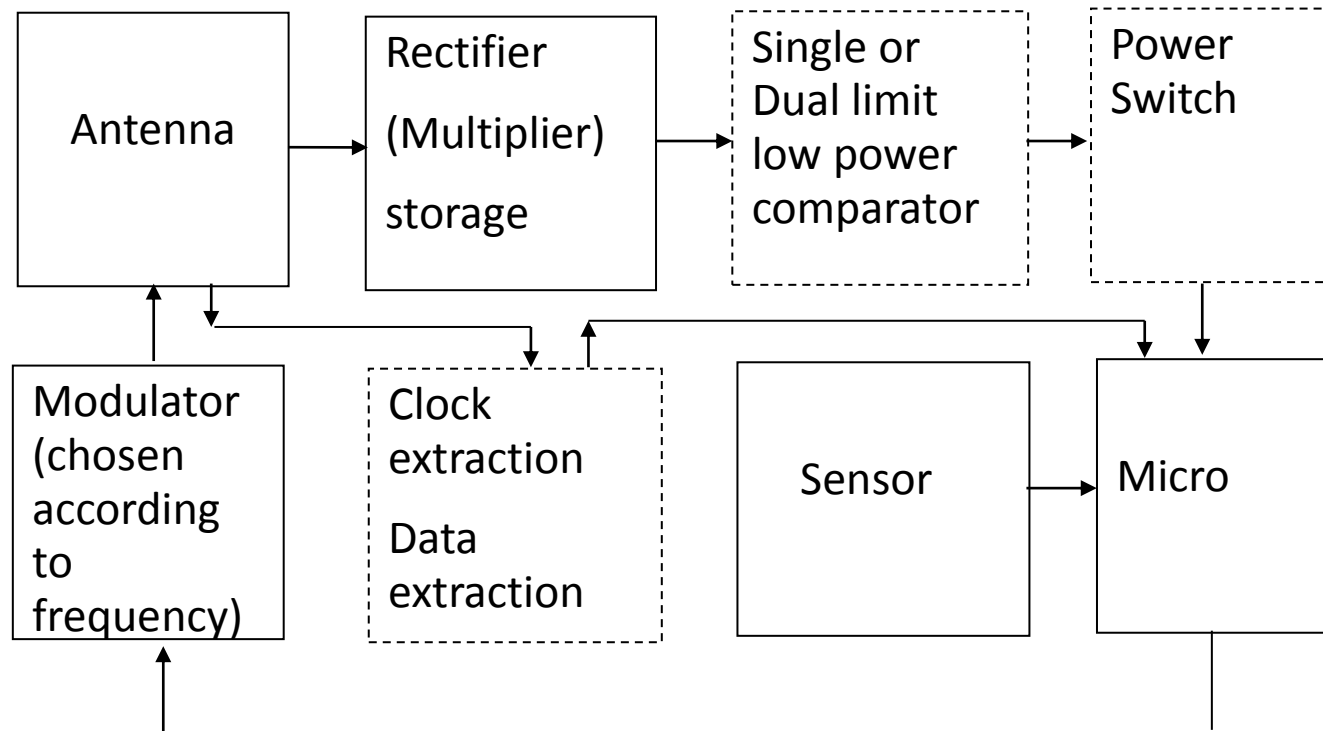
# Case for intelligent and passive RFID sensors

- Introduces flexibility
  - Different types of sensors possible (no dedicated chips)
  - Microcontroller can enhance sensing (e.g. Averaging, filtering)
  - Adaptation to different RFID protocols (load new programs)
- Allows emulation
  - Emulation of RFID protocols (check robustness, speed ,anti-collision schemes, ...)
  - Passive emulation (nearer to real product), smaller size, cheaper
- Enhances security
  - Use of processing power to implement better security (compared to state machines)

# Challenges to overcome in order to realise intelligent and passive RFID sensors

- Low power consumption is critical (also for sensor)
- Harvest and store energy, power management
- Choice of the microcontroller is critical
  - Enough processing power to implement needed schemes
  - Energy requirements should be low (also at start up)
  - Good power saving modes
  - Low voltage is an advantage (1.8 v or lower)
  - Fast wake-up from power saving modes and interrupts
  - Enough timing precision for reliable communications
  - Enough memory to allow implementation of protocols
  - Low power non-volatile
  - Good interfaces for sensors

# µcTag HW: system block diagram



## µcTag HW: EM6819 microcontroller

- Works from 0.9V– 3.3V (allows gains in distance)
- Uses internal multiplier to run between 0.9v and 2v
- CoolRISC CPU, 7.5 Mips at 15 MHz (more processing power if needed)
- Specs typically 140uA @ 1 Mips (3V) better than most micros
- Timers (can be used for modulation, timing)
- Wake up counter (can be used for energy accumulation)
- ADC (for Analog sensors that can live with 10 bits)
- 16K Flash (emulation of identity, protocols, ...)
- EEPROM Emulation, SPI
- Easy to use serial programming and debugging interface

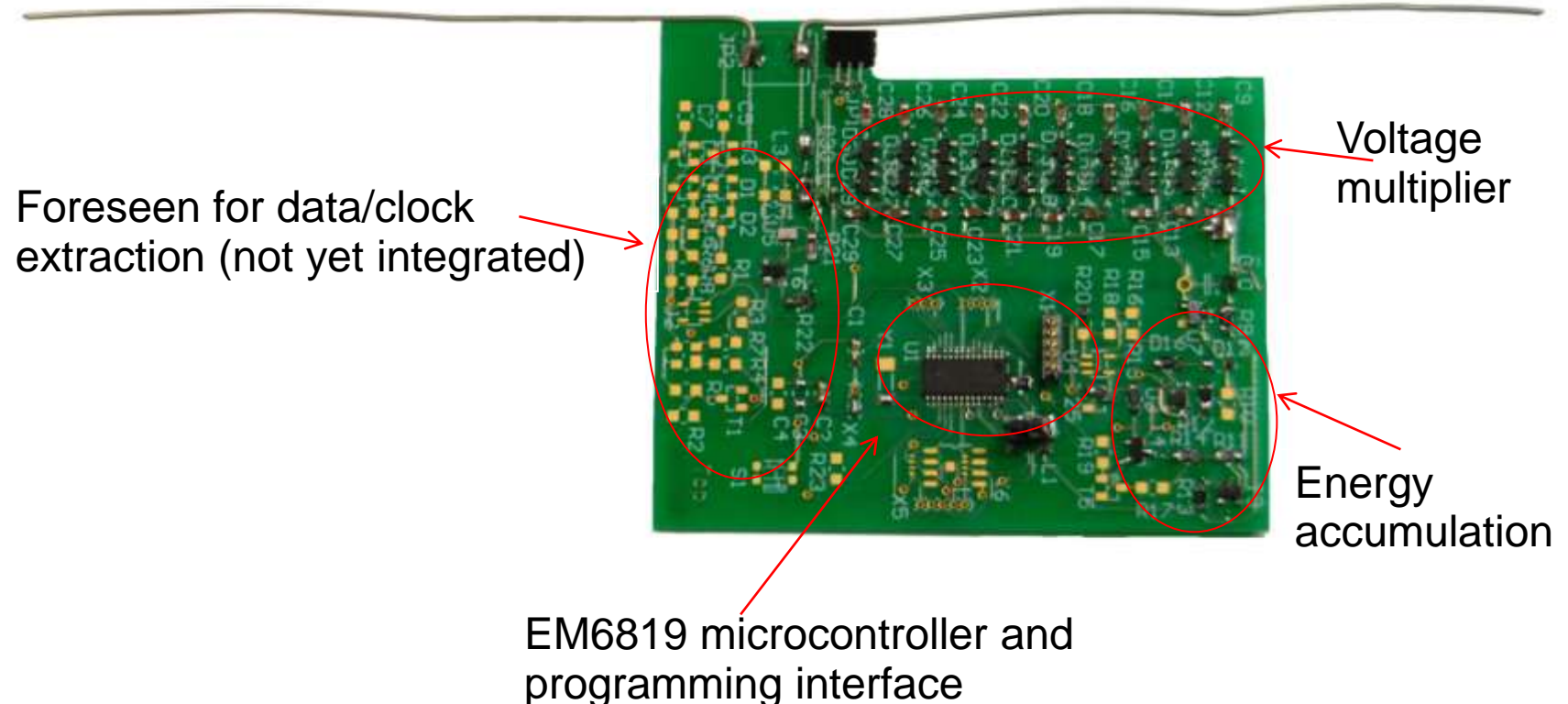
## µcTag HW: EFM32G230F128 micro

- Very low power 32-Bit micro from Energy Micro
  - The EFM32G230F128 is a new low-power microcontroller
  - Very low current consumption in different modes
  - Available with several Flash/RAM sizes (32K ... 128K)
  - Powerful industry standard Cortex M3 architecture
  - Analog and digital interfaces for different sensors
  - Too many features to name. Check datasheet yourself
  - The silicon we used (available in early 2010) still had some bugs and problems. Resulting in non optimized routines in our software
  - Many examples and demos were not yet available during the project phase.

## µcTag First generation HW with EM6819

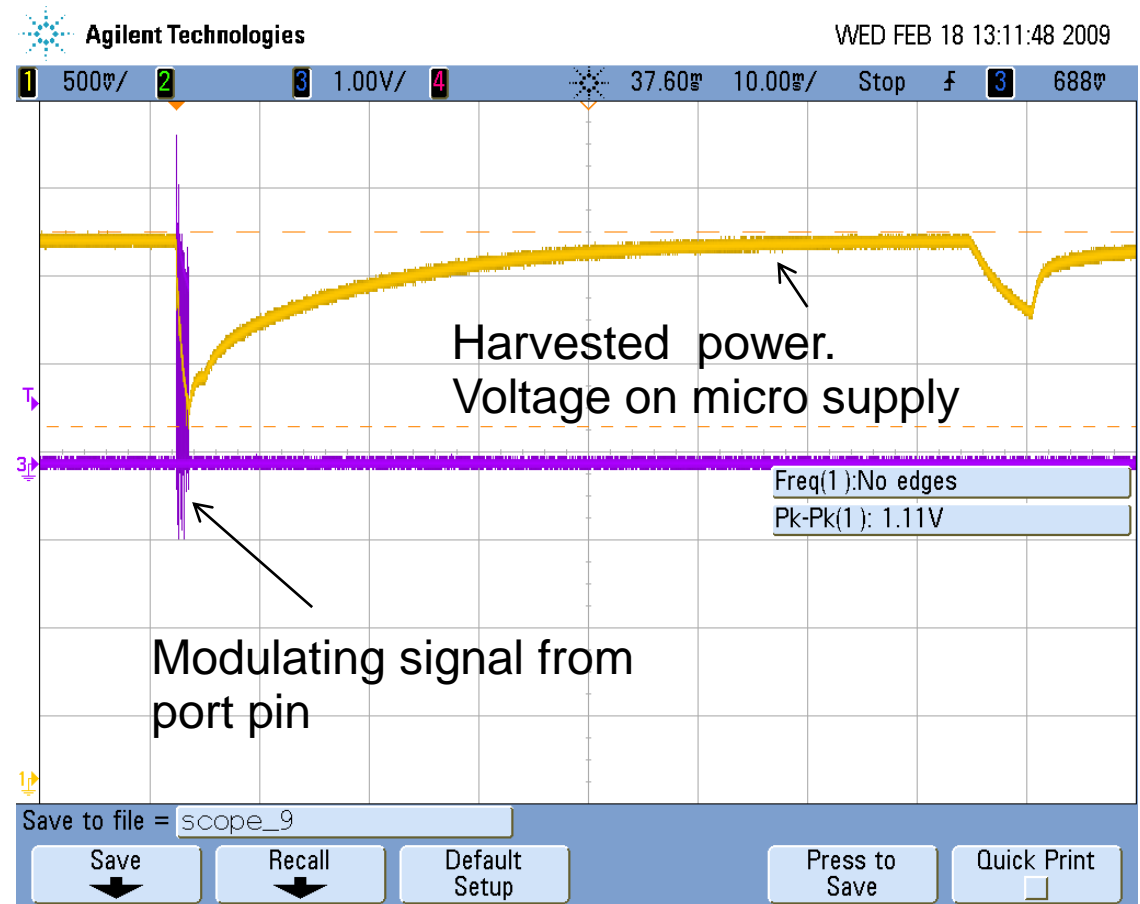
- Emulation of EM1222 tag (868 MHz, Data as 64-Bit ID, sent to reader at 256Kb/S, Micro needs 50µA running at 500KIPS)

868 MHz dipole antenna



## $\mu$ cTag First generation results

- Tag at 2m from reader (500mW). 147nF buffer capacitor used to clearly show the changes on supply
- The Micro sends the identity (or id + sensor data) and then goes into sleep mode.
- During sleep, the supply rises again



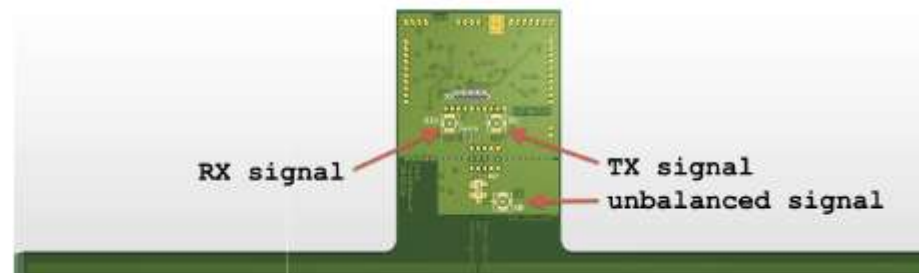
## µcTag First generation results

- Tag at 2m from reader (500mW). 147nF buffer
- A better view of the modulation sequence
- The voltage sinks as the tag starts to send its information. The sending last about 1.2 ms. The energy is more than enough to send the data, even while using such a small capacitor as buffer



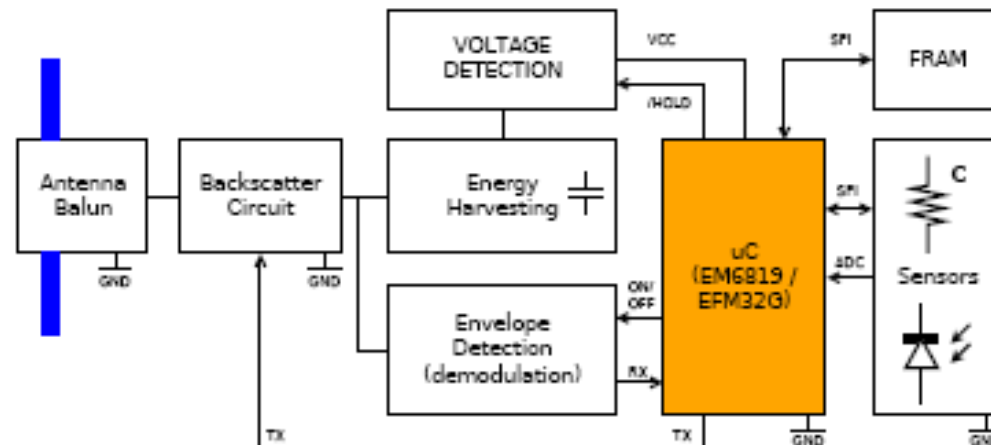
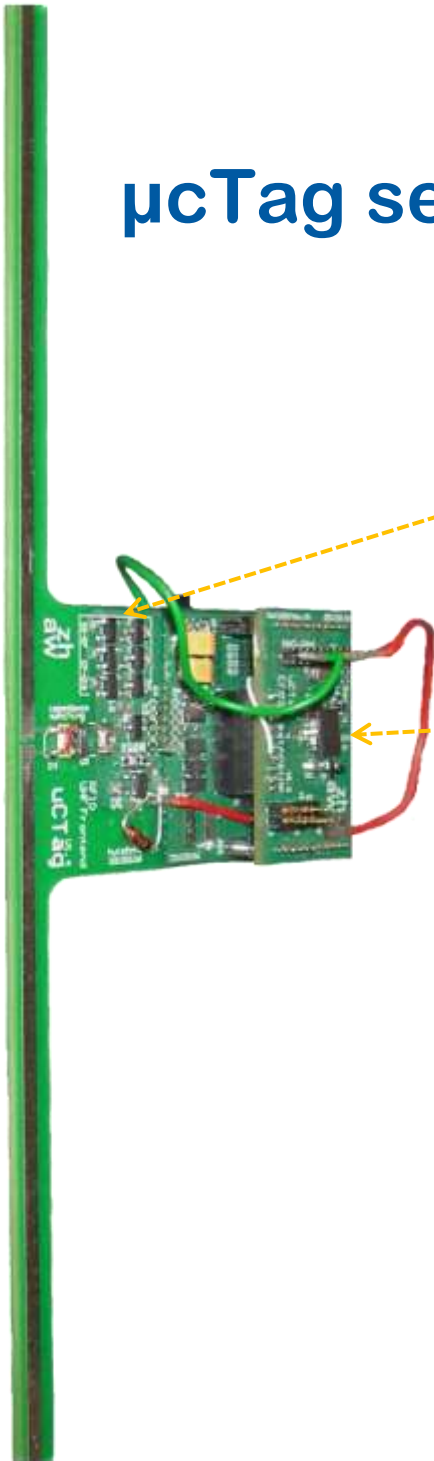
# µcTag second generation

- Motivation
  - First generation limited, especially for complex protocols
  - Micro with fast reaction time and more processing power needed
  - Improvement of energy harvesting and power management
- 2 Boards solution: Flexibility. Allows different microcontrollers.
  - Base board for Energy harvesting and management
  - Piggy board for Microcontroller



# µcTag second generation

- Hardware (Base board + Piggyback)
  - Charge Pump
  - Energy storage
  - Piggy Board with EFM32G230F128 microcontroller
- Software-based signal processing to emulate UHF protocol

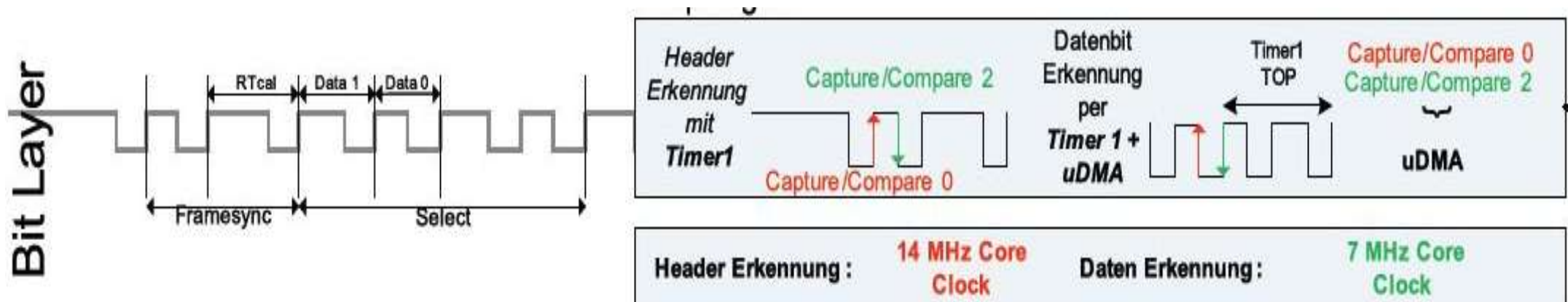


## Some difficulties for complex protocols

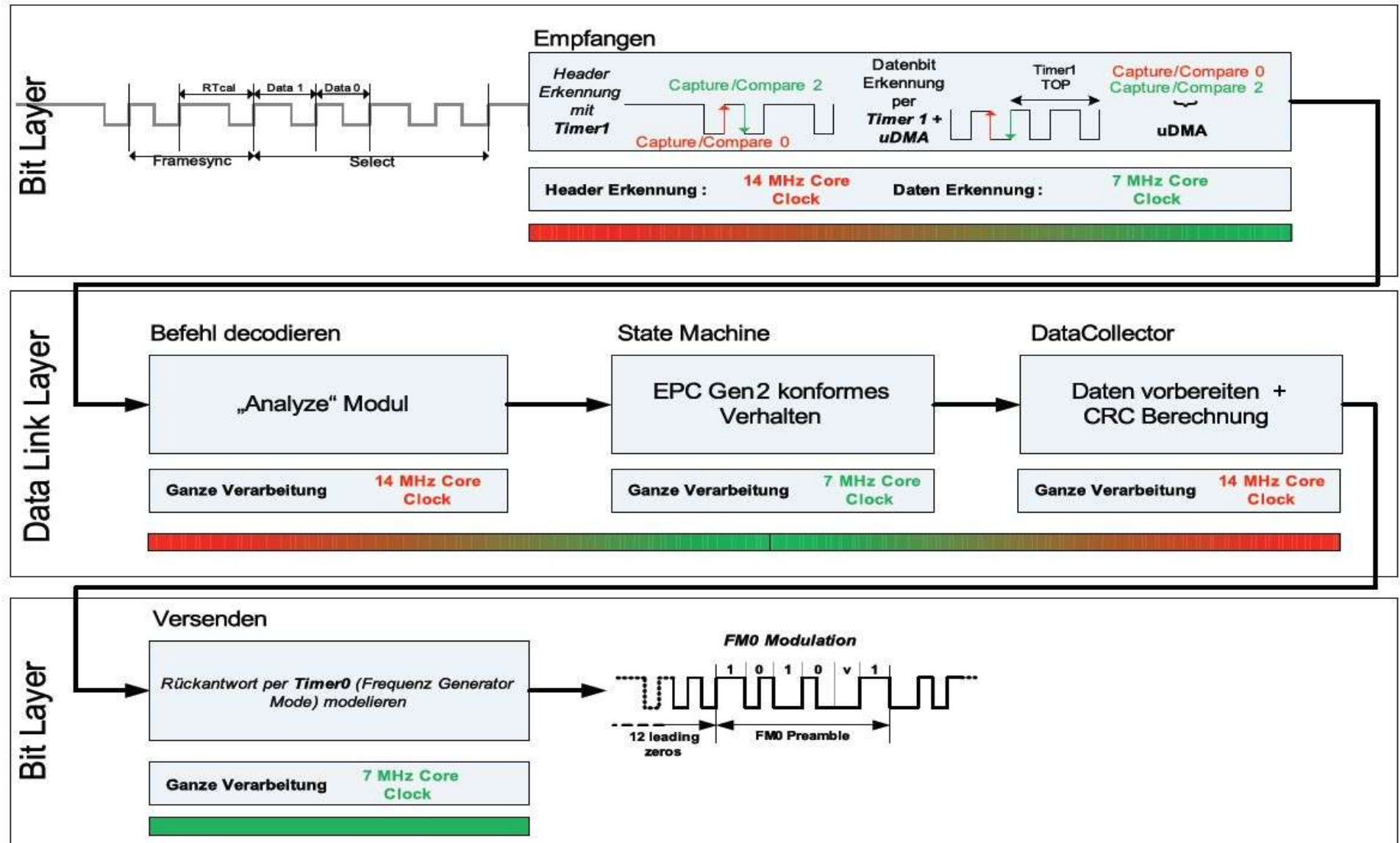
- Some important EPC Gen2 protocol requirements
  - Short reaction time (worst case: 12.5 $\mu$ s)
  - Complex CRC calculation
  - Heavy payload
    - Inventory : 18 Bytes
    - Read Command for the TID membank : 34 Bytes
- EPC Gen2 Collision detection
  - The collision detection is very useful but the additional effort needs more time and energy.

## Difficulties with complex protocols

- Regularly sample the incoming signal with little energy
  - Detect the synchronization, headers
  - Measure times
  - Make required calculations for bit rate
  - Calculate CRCs when needed
  - Decode commands and send answers
  - The combination of timers, DMA, CPU of the EFM32G230F128 proved very valuable for this challenge
- Enough resources/processing power for large programs



# Implementation (Communication example)



## Implementation

- Passive RFID Tag Emulation (Gen2 EM Microelectronic tag emulated)
  - All “Inventory”-Commands implemented
  - All “Read Access” Commands implemented
  - Anti-collision (Slotted ALOHA) implemented
  - Important states implemented (Kill and Open states not implemented)

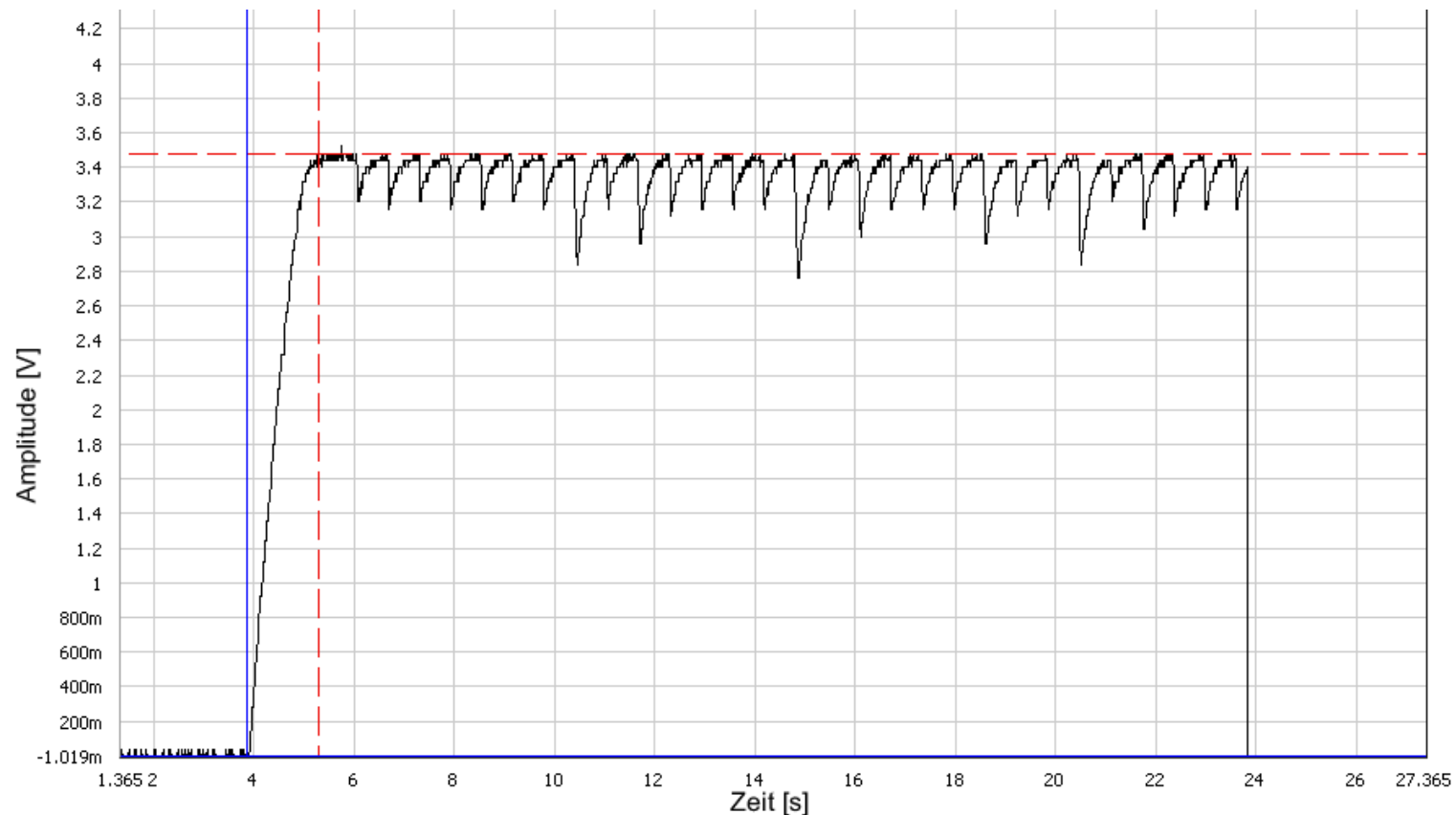
## Setup & results

- Lab reader used for tests (max power 500 mw)
- $\mu$ Tags and RSN Software tested
  - RSN Software to adapt to same tag sending different values
  - $\mu$ cTag (in passive mode)
    - Inventory , Read-Command
    - Anti-Collision
    - Passive tests conclusive until 1.6 m



## Setup & results

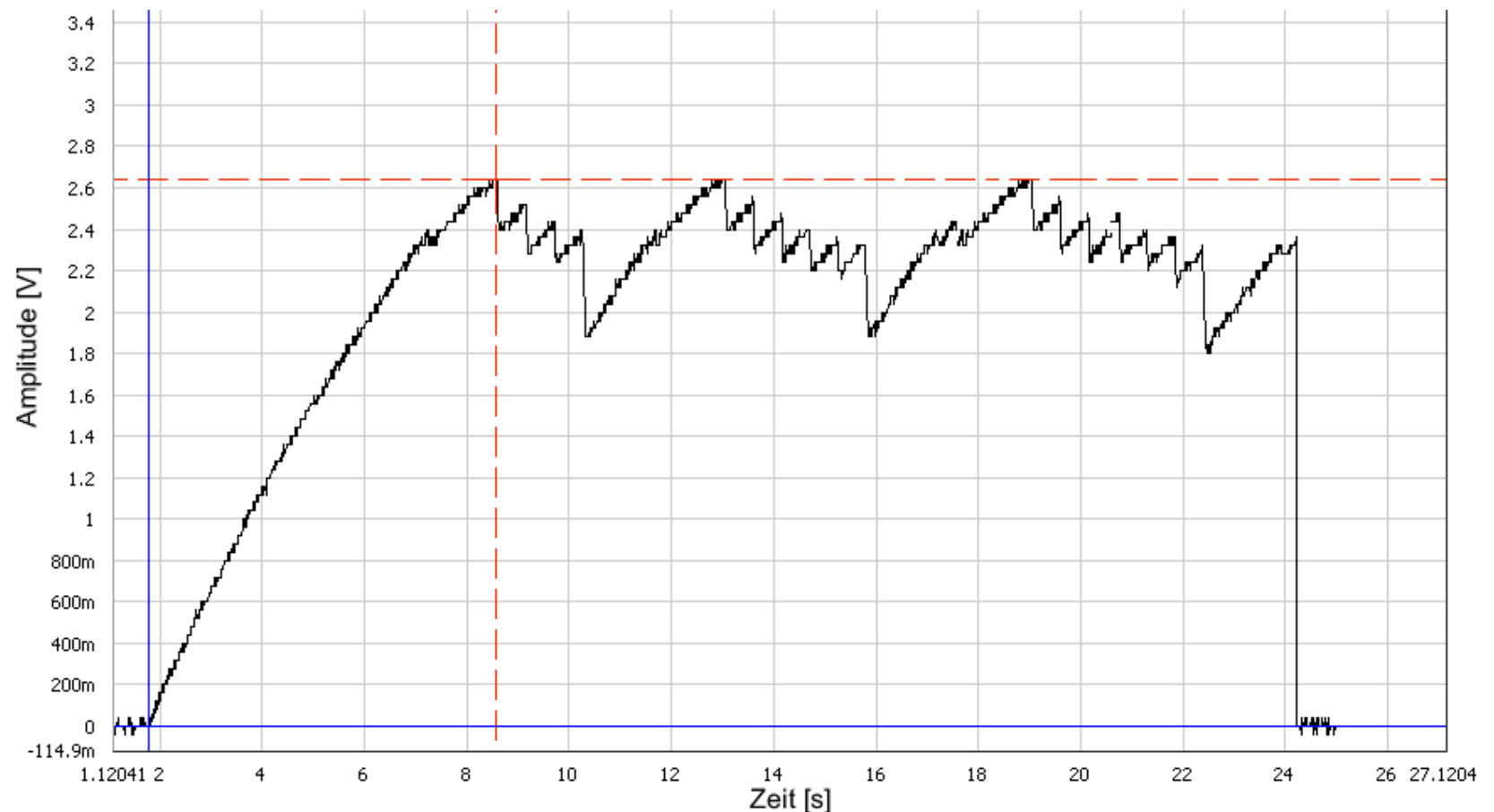
- At 0.2 m (enough energy harvested. Voltage at 2.8V – 3.5 V)



TDS 2024B(CH3)	x1: 3.87	y1: 0	Dx: 1.43	1/Dx: 699.301m
TDS 2024B(CH3)	x2: 5.3	y2: 3.48	Dy: 3.48	Dy/Dx: 2.43357

# Setup & results

- At 1.1 m (harvested voltage down to 1.9V – 2.4V)



TDS 2024B(CH3)	x1: 1.78	y1: 0	Dx: 6.79	1/Dx: 147.275m
TDS 2024B(CH3)	x2: 8.57	y2: 2.64	Dy: 2.64	Dy/Dx: 388.807m

## Setup & results

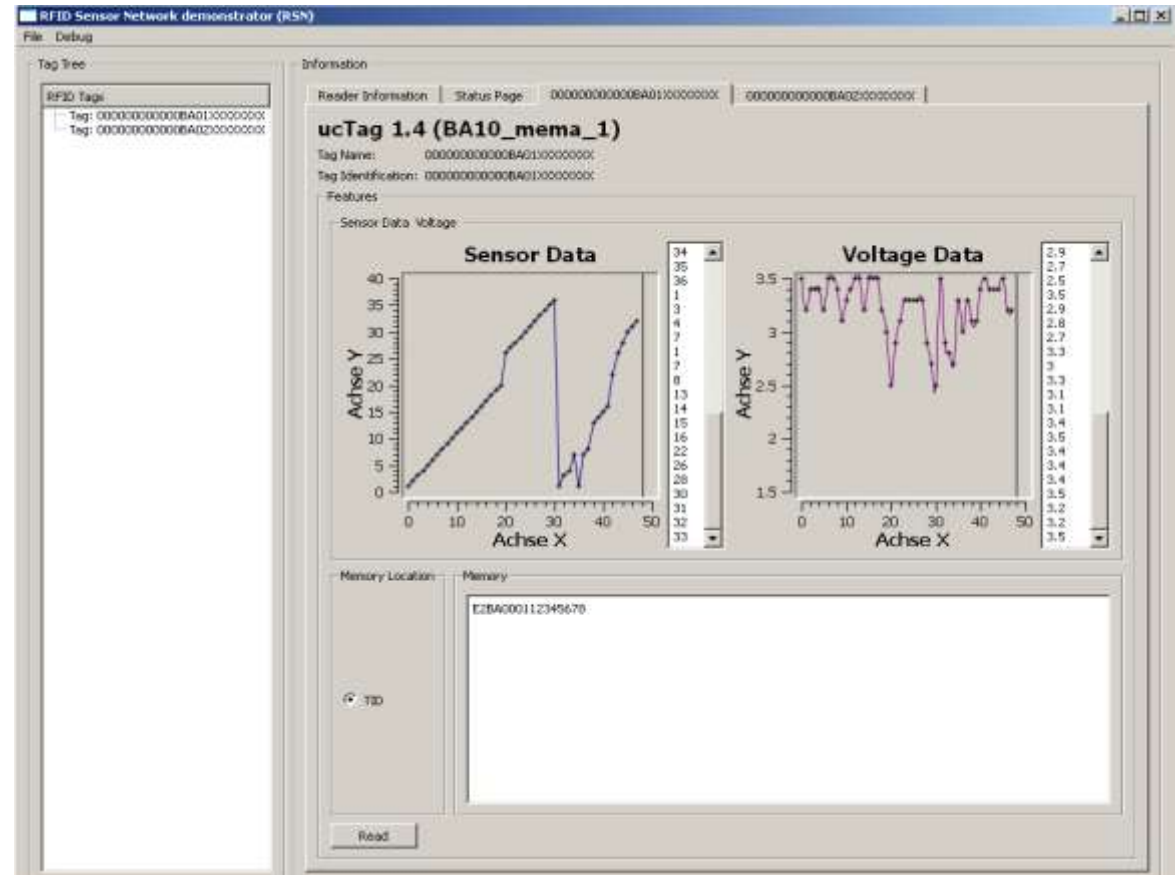
- Zoom at 1.6 m (harvested voltage down to 1.9V – 2.4V)



TDS 2024B(CH3)	x1: 9.96	y1: 2.48	Dx: 1.81	1/Dx: 552.486m
TDS 2024B(CH3)	x2: 11.77	y2: 1.92	Dy: -560m	Dy/Dx: -309.392m

# Results

- Data captured and displayed using a RSN software developed in the project
- Wide operating range up to 1.6 meter
- Internal counter used to simulate sensor



## Battery supported Operation

- In case of Semi-Passive Operations with battery support
  - CR2032 Li-Mn, 3V used
- Type of application 1: (Inventory-Rounds without sleep)
  - Inventory, Frame Length 8.6ms, polling-mode
  - Result: 5 days
- Type of application 2: (Inventory-Rounds every minute)
  - Inventory, Frame Length 8.6ms, Sleep Time: 1 minute, polling-mode
  - Result: 20 years



## Conclusions

- We have shown that it is possible to passively emulate RFID tags using low power microcontrollers. The emulated tags can be fitted with different sensors, eliminating the need to develop a new chip for every other sensors. Furthermore, the presence of intelligence allows pre-processing functions and better security
- For easy protocols, a low-power 8-bit microcontroller such as the EM6819 will do
- For complex protocols, the low power 32-bit microcontroller of Energy Micro is a very good choice.

## Future work

- The one and only existing 32 bit passive implementation of a RFID Tag (as far as we know)
- Very flexible software design and a module based concept allows to simply extend and modify the software
- Work will continue to deal with the following issues:
  - Implementation other features
    - This is basically energy uncritical software work
    - Newest components for harvesting (better range)
  - Use of a new low power microcontroller with much shorter wake-up times, more energy efficient

## Thanks./ If you need more information

- Thanks to EM Microelectronic Marin for providing components
- Thanks to Energy Micro for providing components/kits
- For more information, contact

Prof. Dr. Marcel Meli, Head of Wireless Systems Group  
marcel.meli@zhaw.ch

Zurich University of Applied Sciences (ZHAW)  
Institute of Embedded Systems (InES)  
Technikumstr. 9  
CH-8401 Winterthur  
Phone: +41 58 934 75 25

# Questions

????

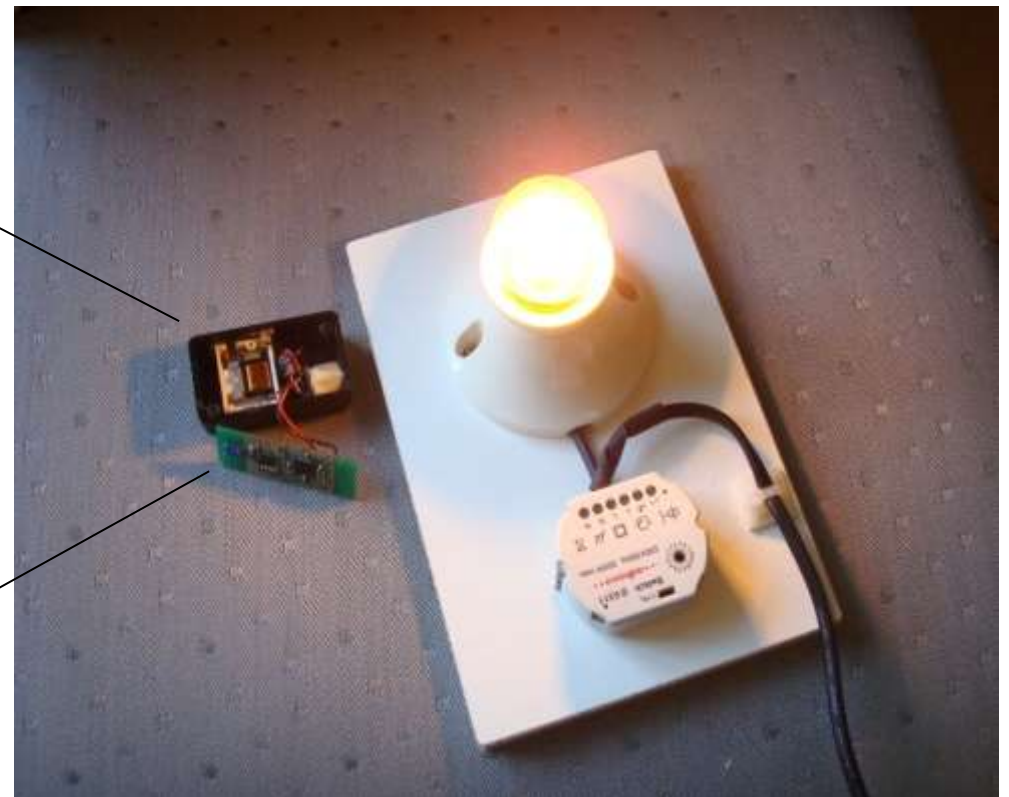
## Who we are + update of our activities.

### ZigBee compatible Wireless Battery-less switch

- Use of electro-dynamic EH module (100 – 200 Micro joules)
- Frames compatible with 802.15.4 / ZigBee (about 30 bytes)



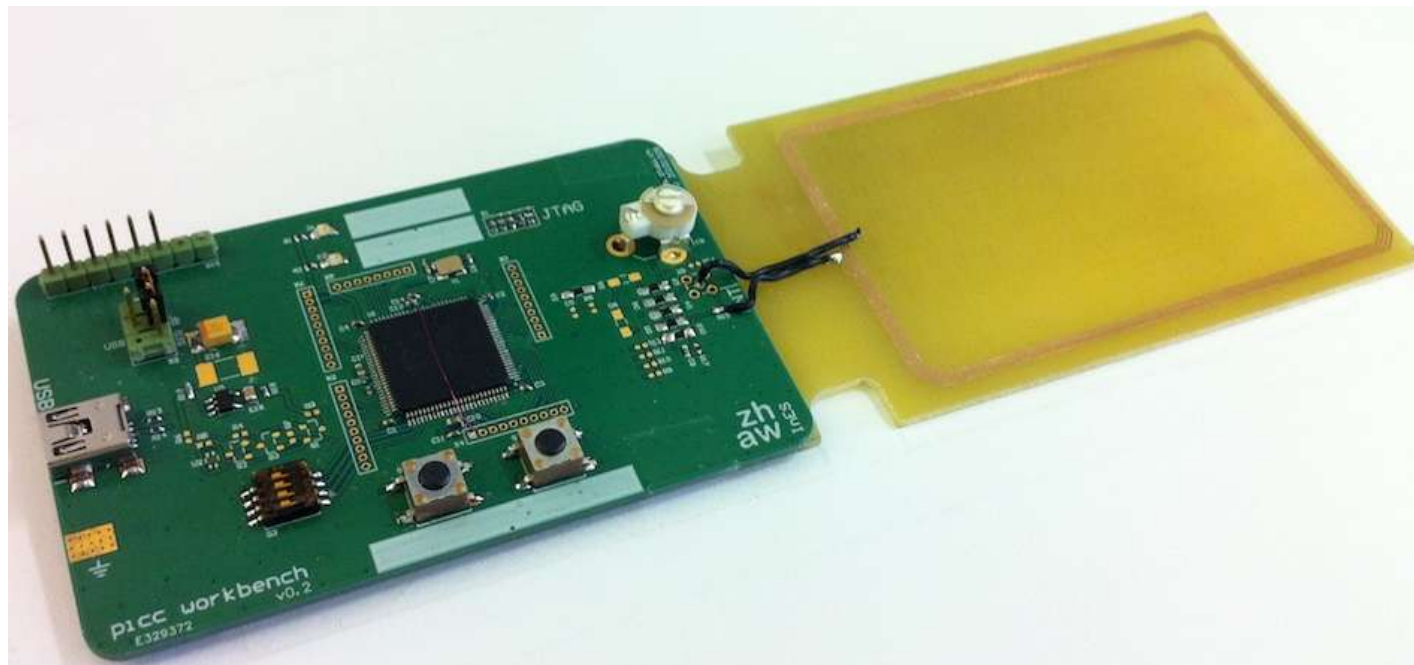
**No Batteries, No maintenance**



## Who we are (our activities in RFID)

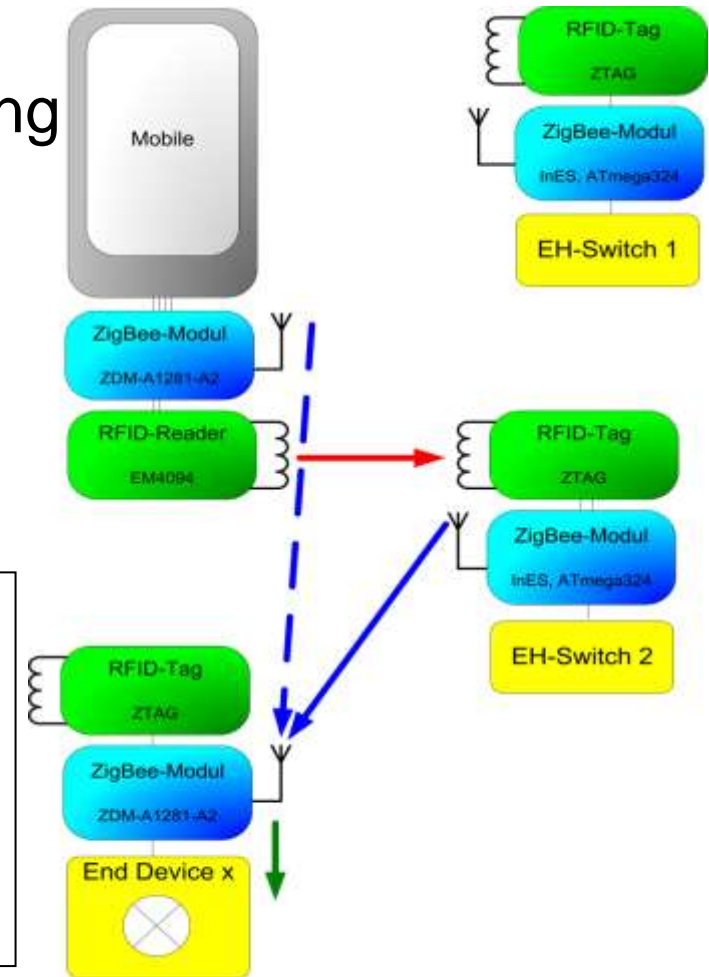
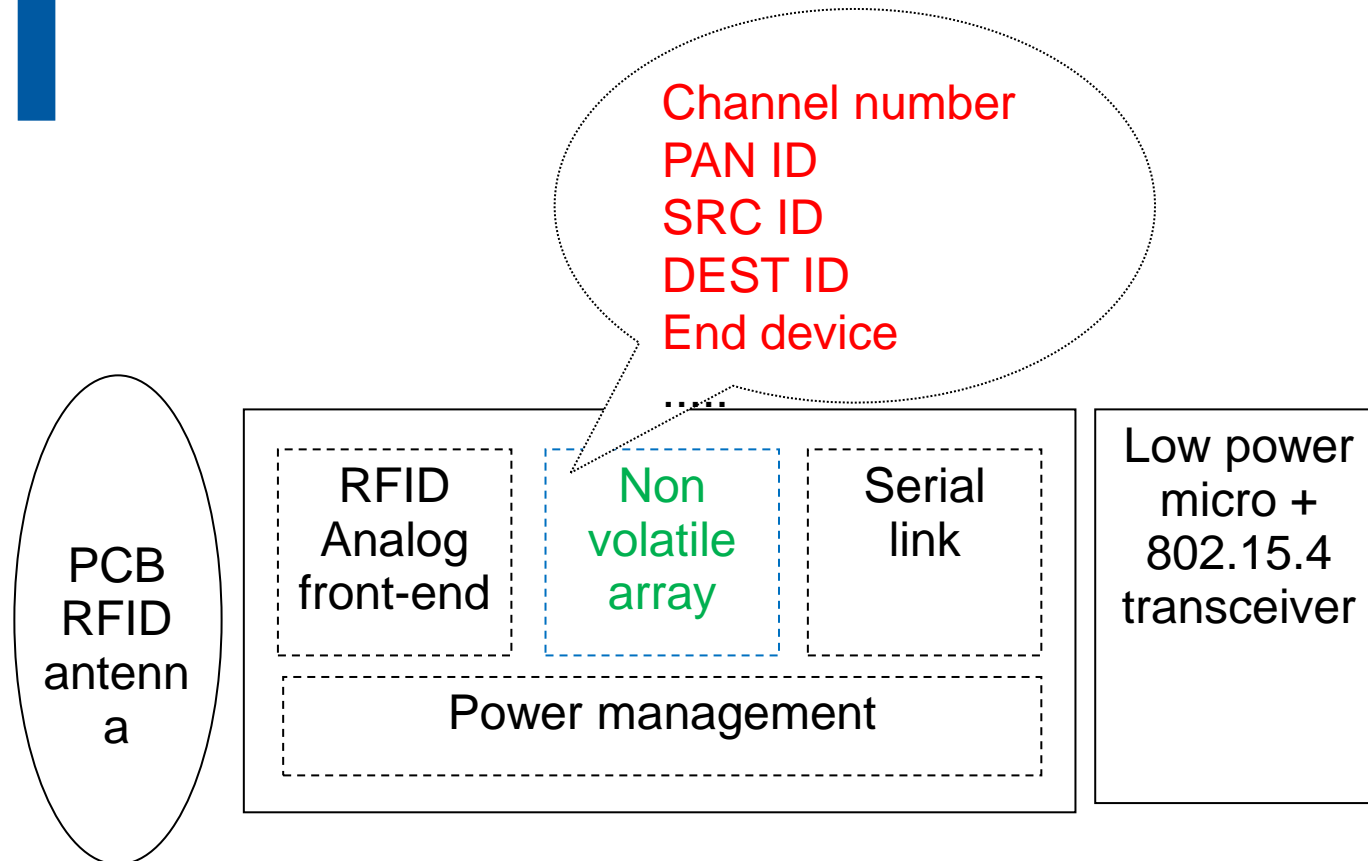
### Emulation of complex HF, LF protocols using a micro.

- Credit card size
- Emulate, sniff, ... ISO14443A implemented



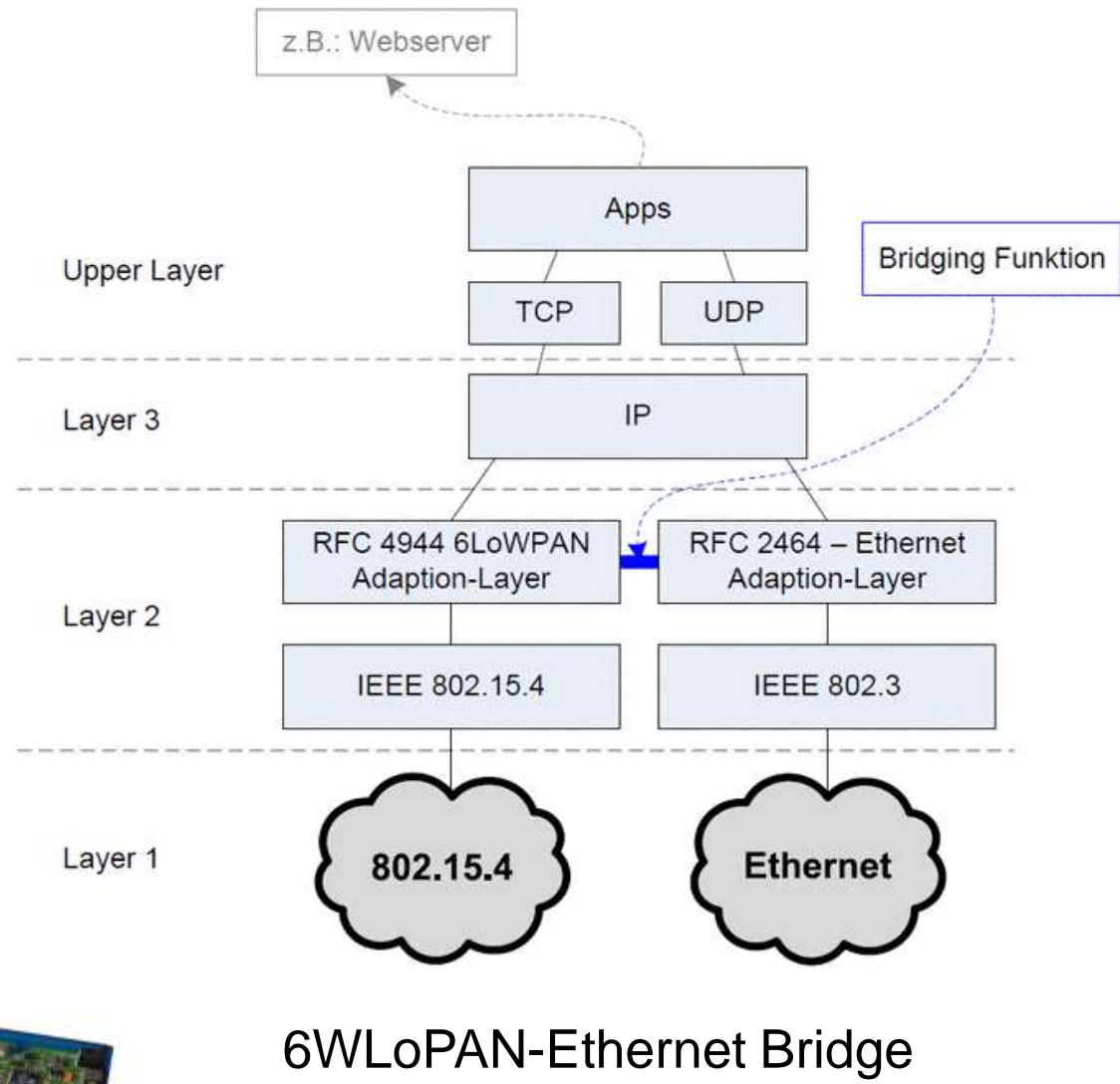
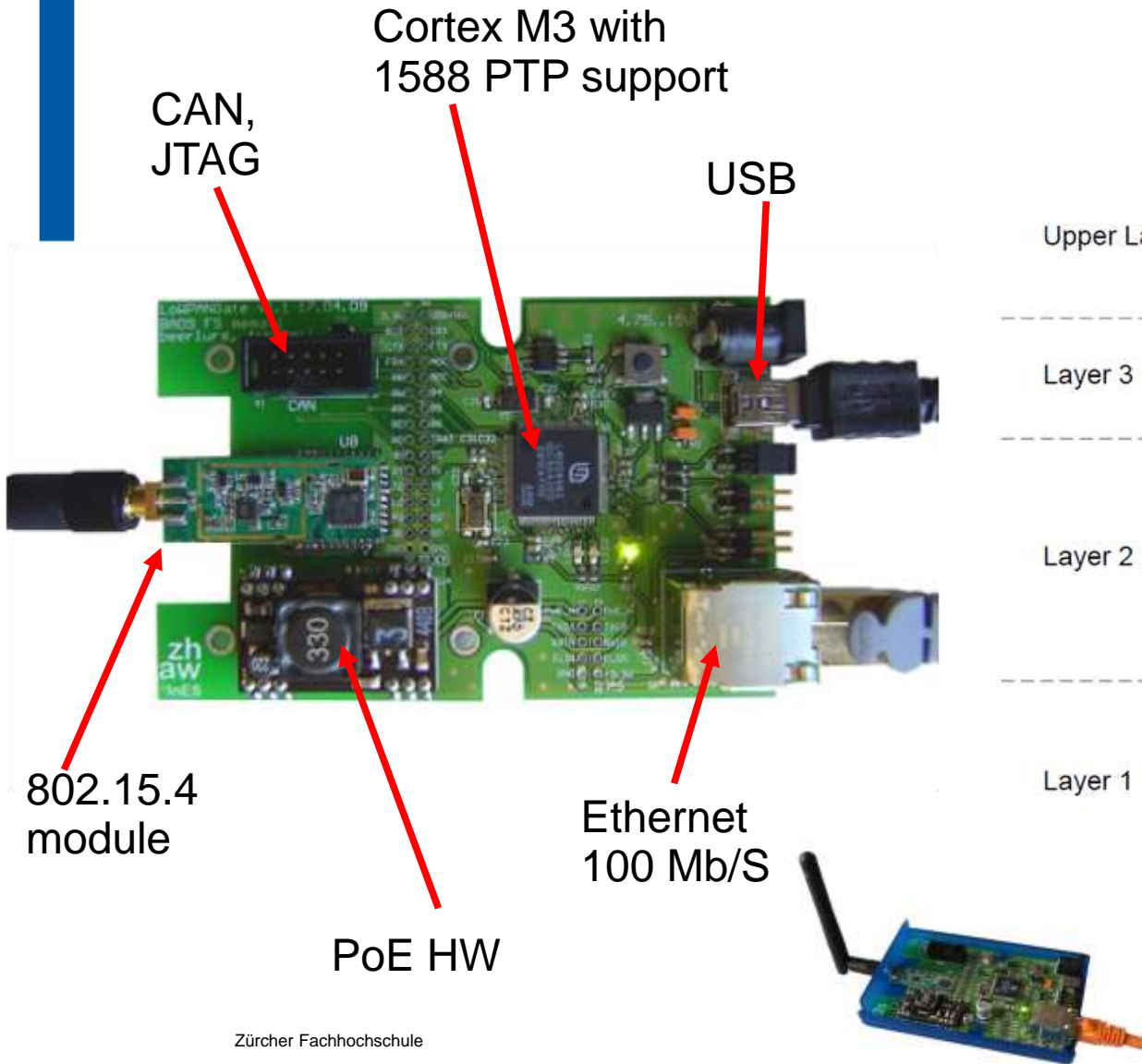
# Who we are (our activities in RFID). Pairing

- ZB used as wireless standard
- Lamp, switch, iPod use RFID for pairing



Using an iPod/mobile phone as pairing tool

# Who we are + update of our activities



# Who we are + update of our activities

## Multichannel sniffer

- Sniff all ZigBee / 802.15.4 channels (adaptable to all bands 2.4 GHz, 868 MHz, ...)
- Linked to PC using Ethernet or USB
- Modular. Adapt to your needs. Better than 1 microsecond resolution

Timestamp	Channel	RSSI	Type	Sniffer	Location
14754.032227	12	-58	Beacon	parsum	testsniffer
14754.093750 (+0.061523)	12	-58	Beacon	parsum	testsniffer
14761.267578 (+7.173828)	12	-57	Data	parsum	testsniffer
14761.329102 (+0.061523)	12	-57	Data	parsum	testsniffer
14956.211914 (+194.882813)	12	-72	Acknowledgm	testsniffer	parsum
14956.274414 (+0.062500)	12	-70	Acknowledgm	testsniffer	parsum
14956.337891 (+0.063477)	12	-70	Acknowledgm	testsniffer	parsum
14963.416992 (+7.079102)	12	-68	Command	testsniffer	parsum
14963.478516 (+0.061523)	12	-69	Command	testsniffer	parsum
14963.541992 (+0.063477)	12	-68	Command	testsniffer	parsum
15014.226563	11	-100	Beacon	testsniffer	parsum
15159.111328 (+144.884766)	11	-67	Command	parsum	testsniffer
15159.174805 (+0.063477)	11	-67	Command	parsum	testsniffer
15159.236328 (+0.061523)	11	-67	Command	parsum	testsniffer

Filter  
Channel: 12  
802.15.4 MAC  
Total Bytes: 4  
Byte[0 - 3]: 03 aa bb cc

A version to sniff all 16/channels exists. Real time communication between modules tens of meter apart possible (accurate time stamp)