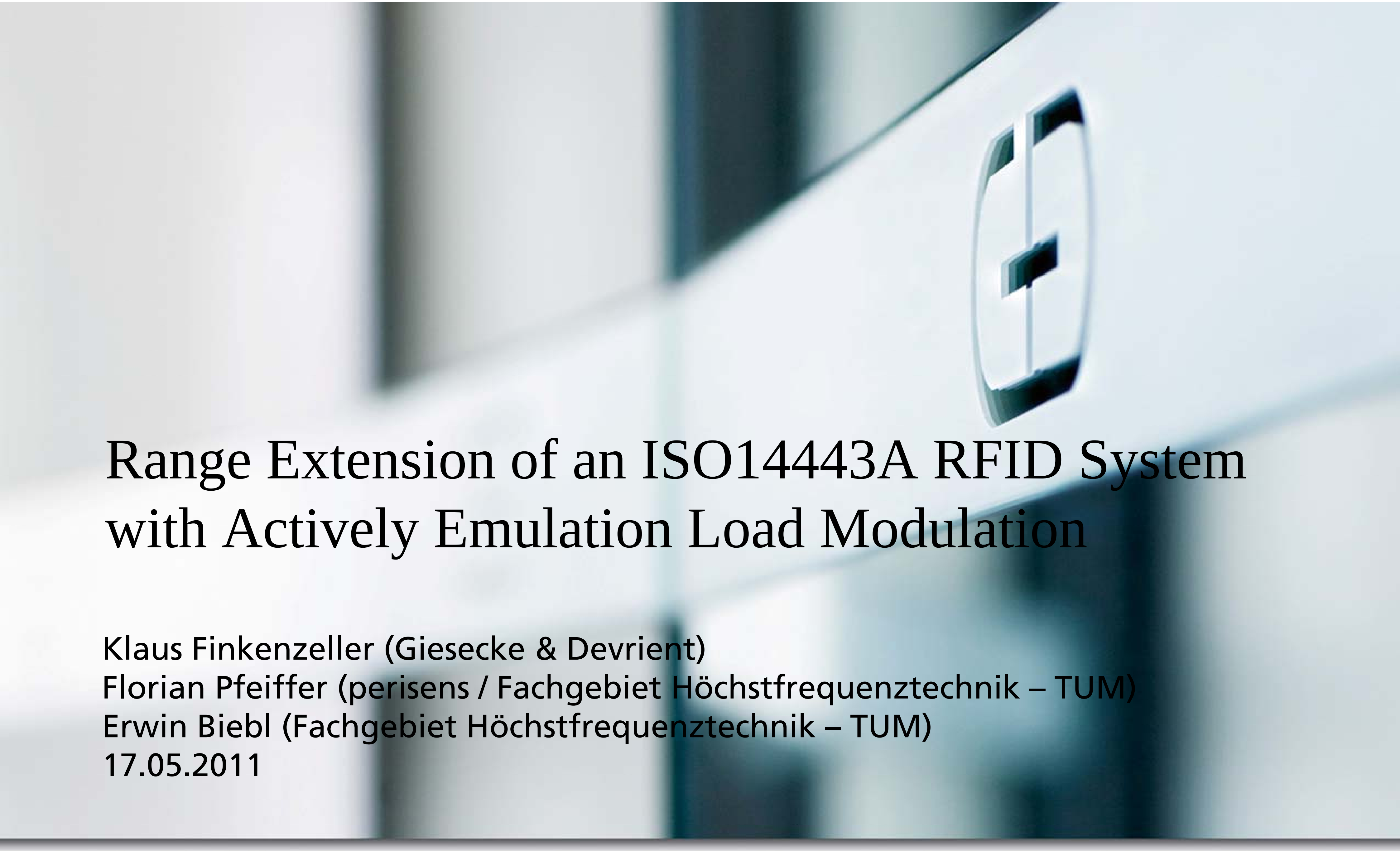


Range Extension of an ISO14443A RFID System with Actively Emulation Load Modulation

Klaus Finkenzeller (Giesecke & Devrient)
Florian Pfeiffer (perisens / Fachgebiet Höchstfrequenztechnik – TUM)
Erwin Biebl (Fachgebiet Höchstfrequenztechnik – TUM)

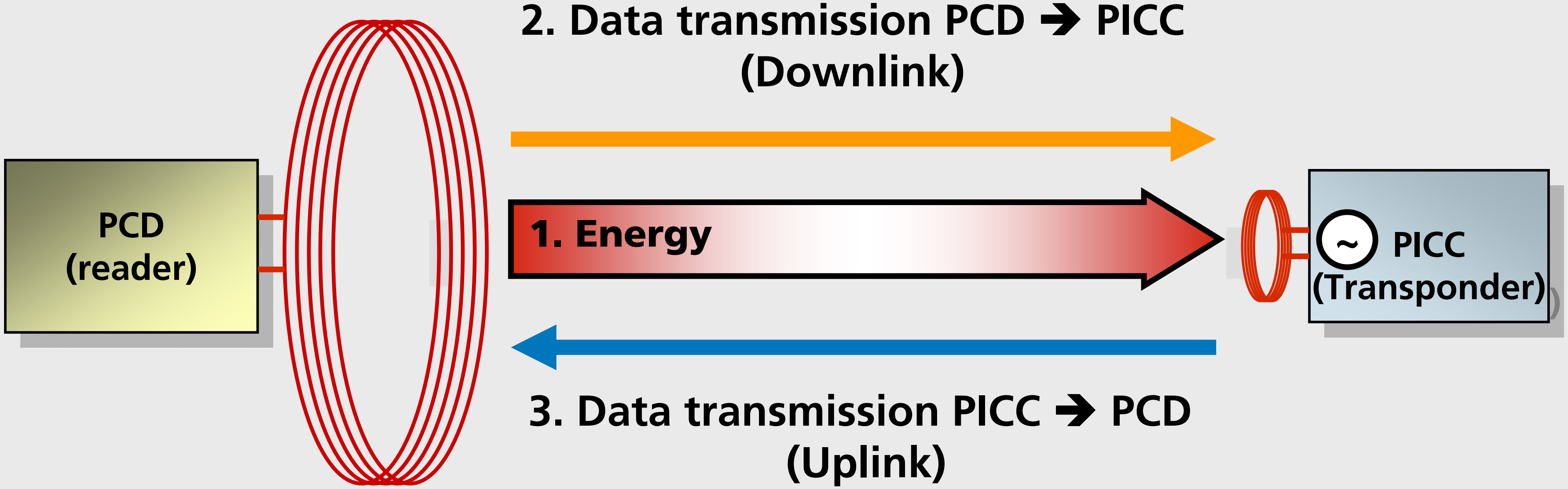
17.05.2011

Motivation

Gaining high reading distances with active load modulation could be used to attack an RFID reader

- Accessing an ISO 14443 reader from much more distance, than the nominal 10 cm
- No limitation in “tags” (PICC) antenna size
  - Useful antenna sizes from 10 cm … 1.5 m in diameter
- No limitation in “tags” (PICC) transmission power
  - 100 W seems to be applicable with no problem
  - Up to 1 kW seems to be possible with improved equipment

Limiting Factors of a Passive Tag System

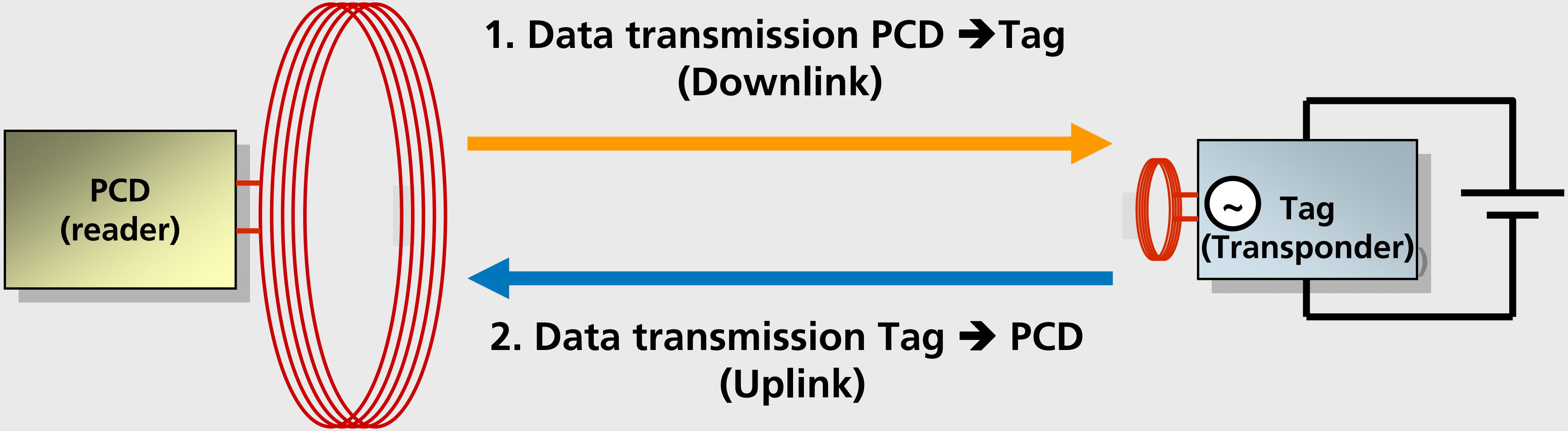

2. Data transmission PCD → PICC
(Downlink)
PCD
(reader)
1. Energy
~
PICC
(Transponder)
3. Data transmission PICC → PCD
(Uplink)

1. Power: The small PICC antenna accumulates not enough energy from the field.

2. Downlink: Coil voltage is too low for demodulation

3. Uplink: The load modulation effect with the small PICC antenna is too poor

Limiting Factors of an Active Tag System



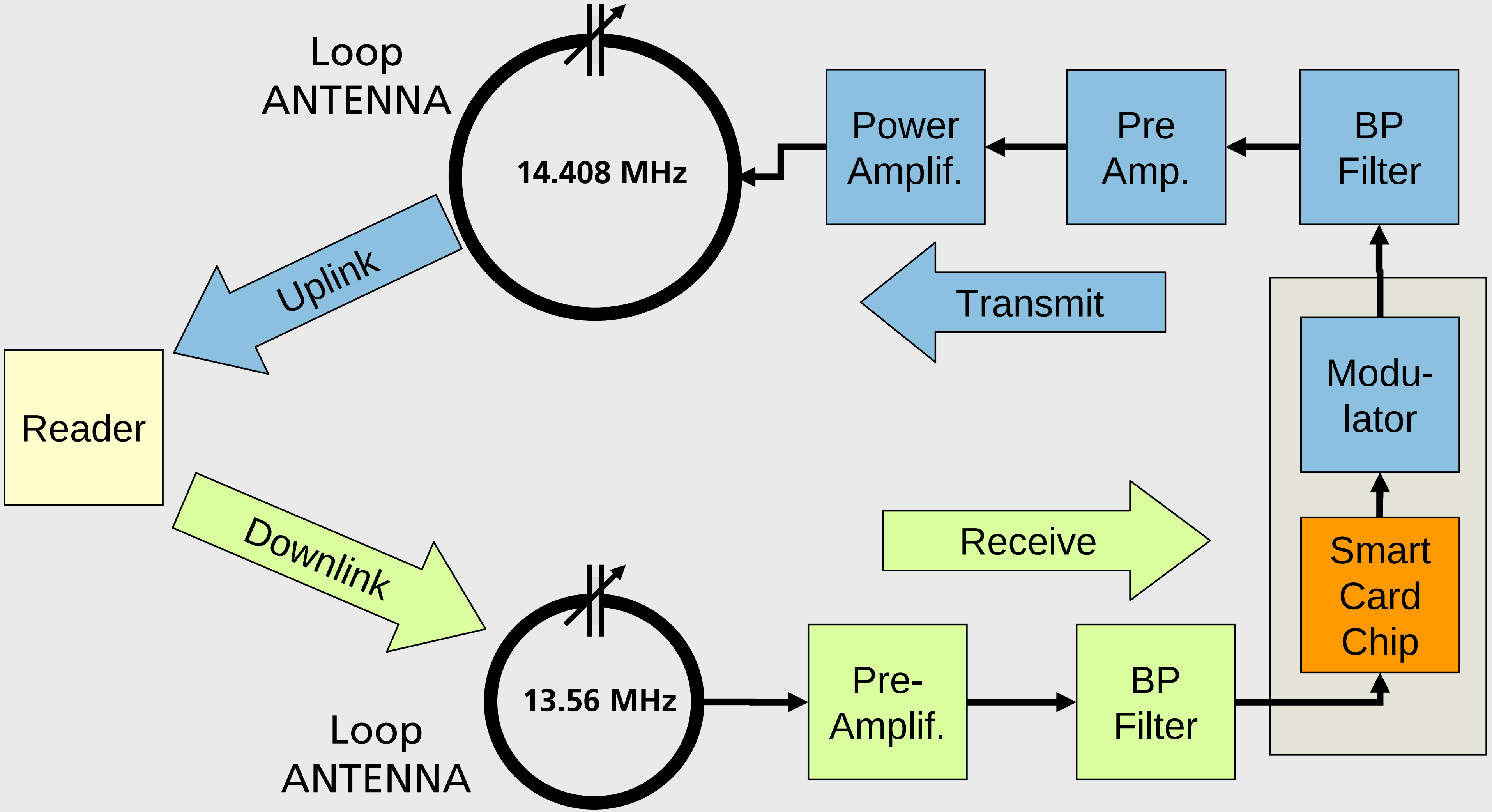
1. Downlink: Transponder coil voltage is too low for demodulation

Solution: improve receiver / noise limited!

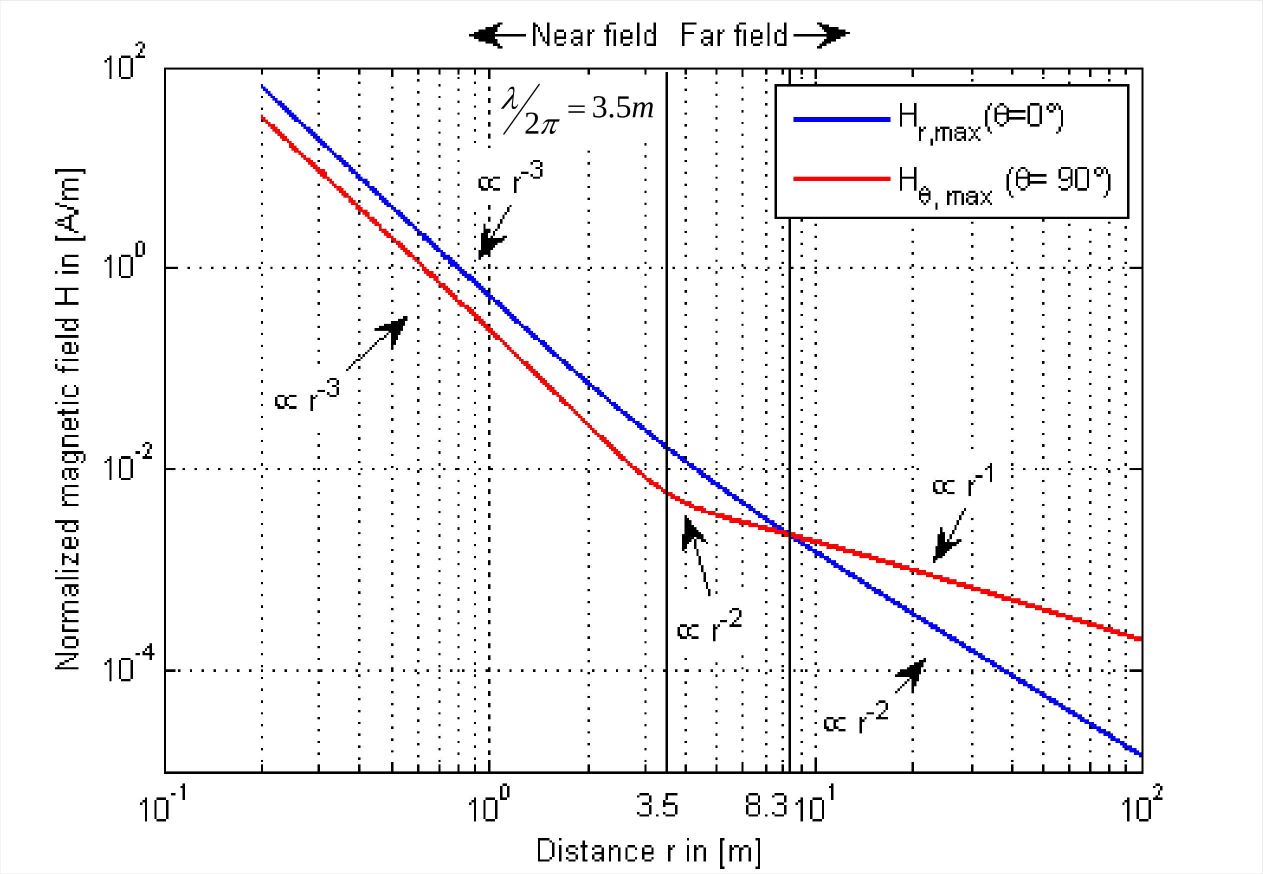
2. Uplink: The load modulation effect with is too poor

Solution: increase magnetic field!

Prototype Implementation



Small circular loop antenna

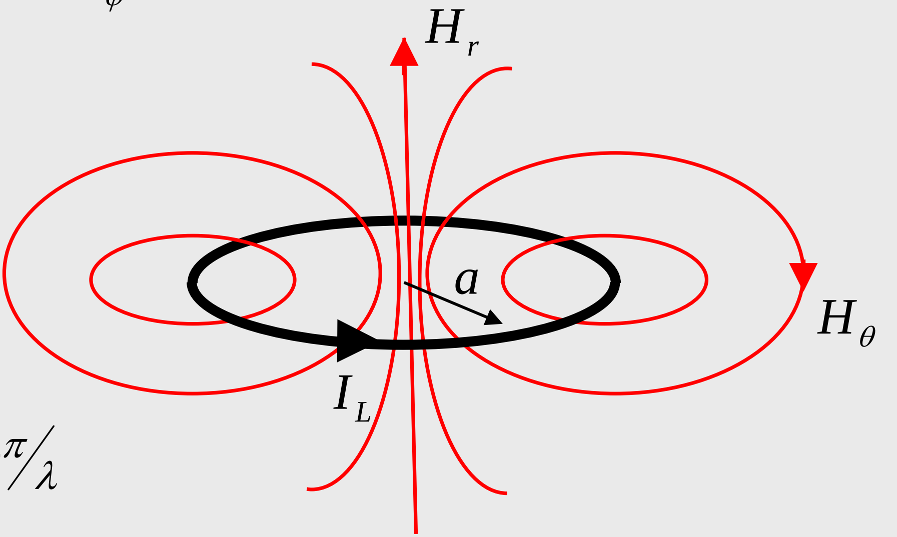


Magnetic fields:

$$H_r = j\frac{ka^2 I_L \cos\theta}{2r^2}\left(1+\frac{1}{jkr}\right)e^{-jkr}$$

$$H_\theta = j\frac{(ka)^2 I_L \sin\theta}{4r}\left(1+\frac{1}{jkr}-\frac{1}{(kr)^2}\right)e^{-jkr}$$

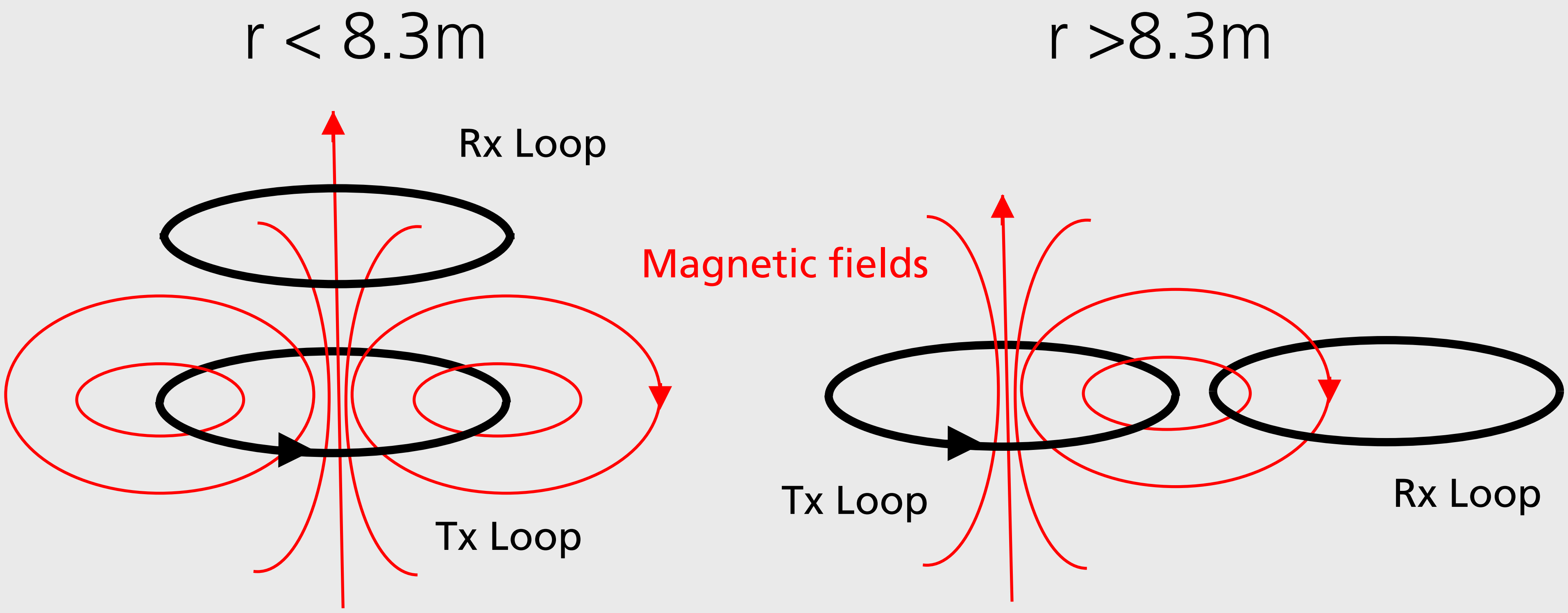
$$H_\varphi = 0$$



Legend:

a… loop radius, I_L … loop current, k… wavenumber $k = 2\pi/\lambda$
r… distance

Loop Placement

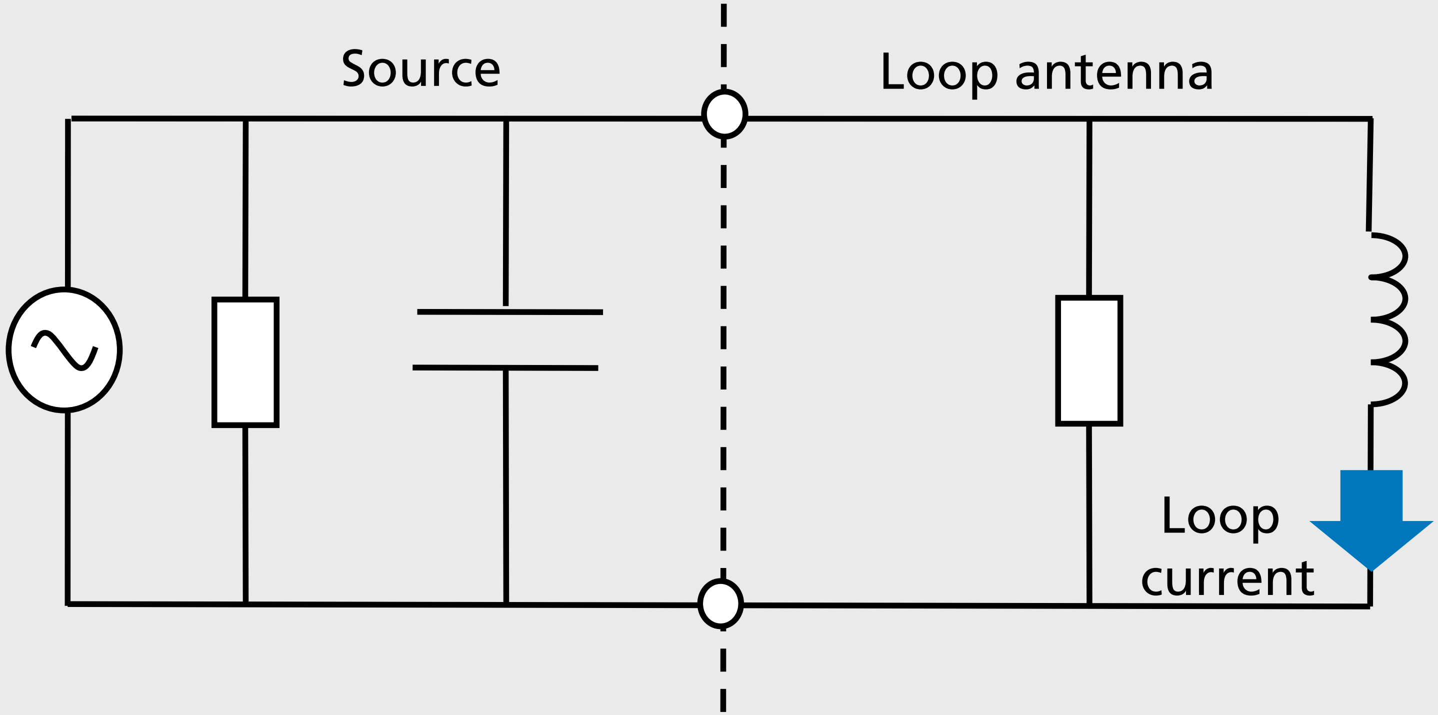


Coaxial orientation

Coplanar orientation

Technische Universität München
Giesecke & Devrient

Active tag in transmitting mode



Circular loop antenna:

$$L = \mu a\left(\ln\left(\frac{8a}{b} - 2\right)\right)$$

Power

$$Q = \frac{1}{\text{3dB - Bandwidth}}$$

$$I(\omega = \omega_r) = \sqrt{\frac{2PQ}{L\omega_r}}$$

Inductance

Resonance frequency

Influencing Factors

	Magnetic field	Tx range (near field: $H \sim 1/r^3$)
A… Area enclosed by the loop	$H \sim A^{3/4}$	$r_{\max} \sim \sqrt[4]{A}$
P… Transmit power	$H \sim \sqrt{P}$	$r_{\max} \sim \sqrt[6]{P}$
Q…Quality factor	$H \sim \sqrt{Q}$	$r_{\max} \sim \sqrt[6]{Q}$

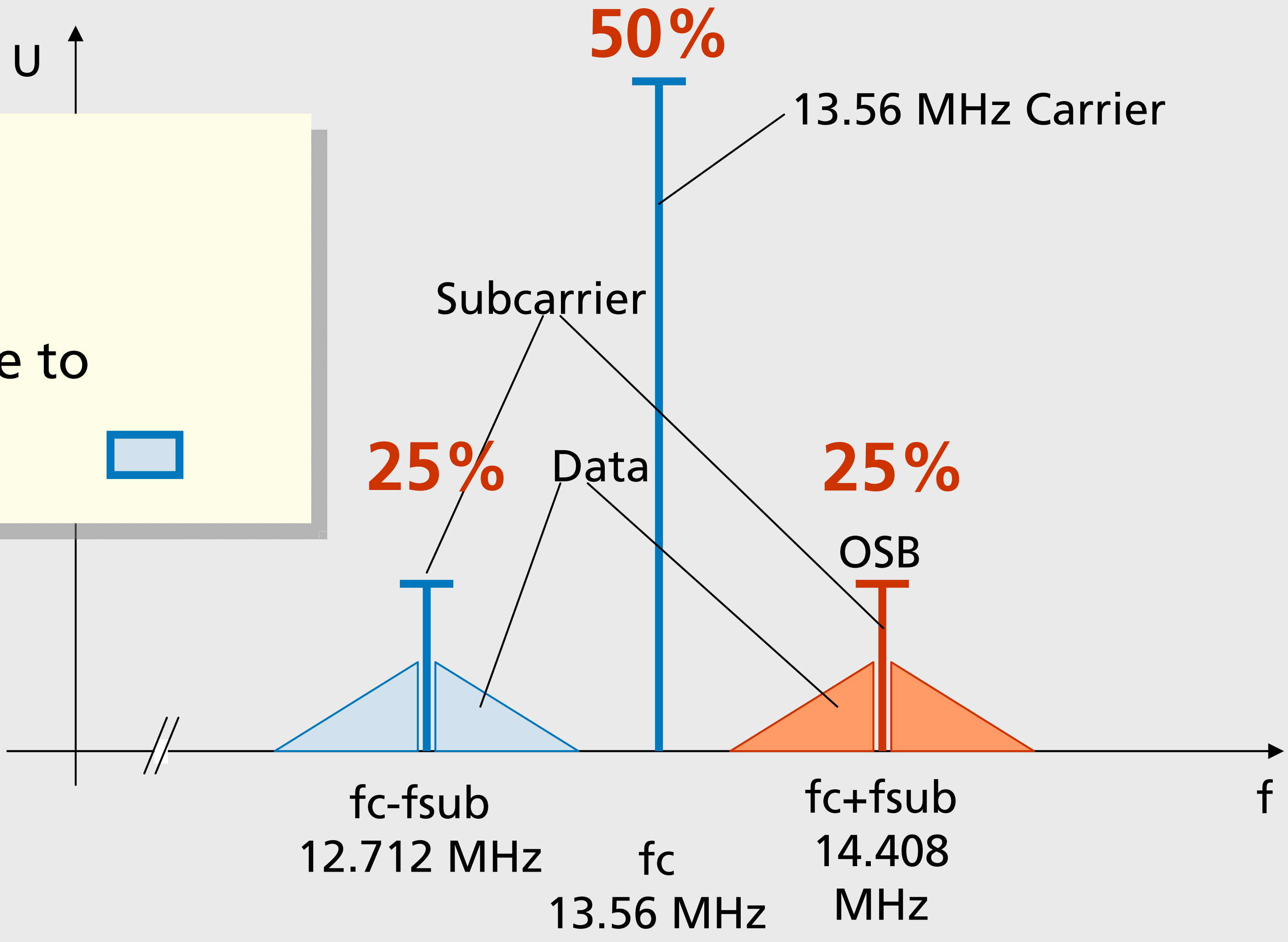
Increase Tx range by 100%, requires…

- ➔Increase loop area by a factor of 16
- ➔Increase power by a factor of 64
- ➔(Increase quality factor by 64)

Maximizing Tx Power

Without filtering:

75% of Tx power will not contribute to communication

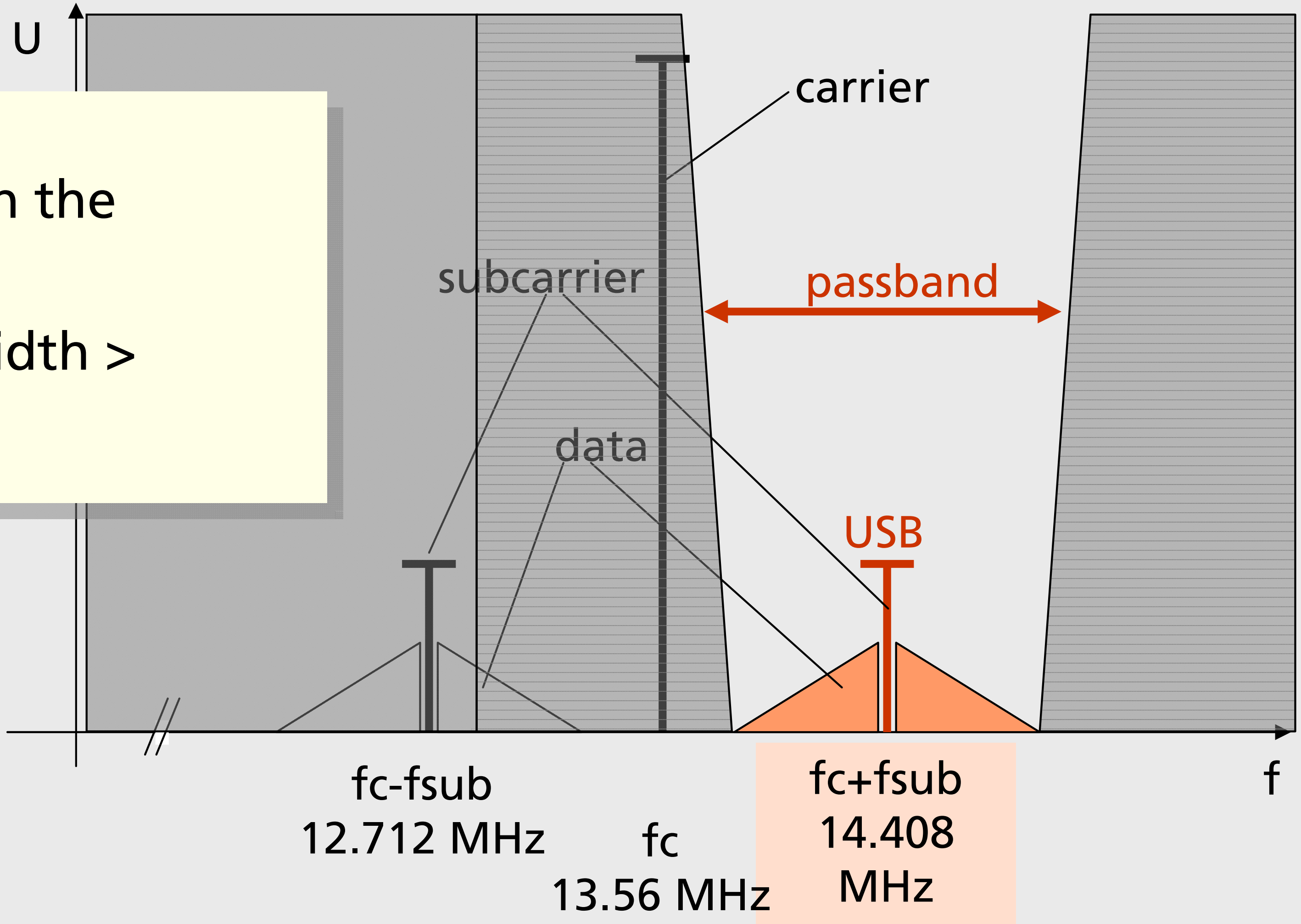


Maximizing Tx Power

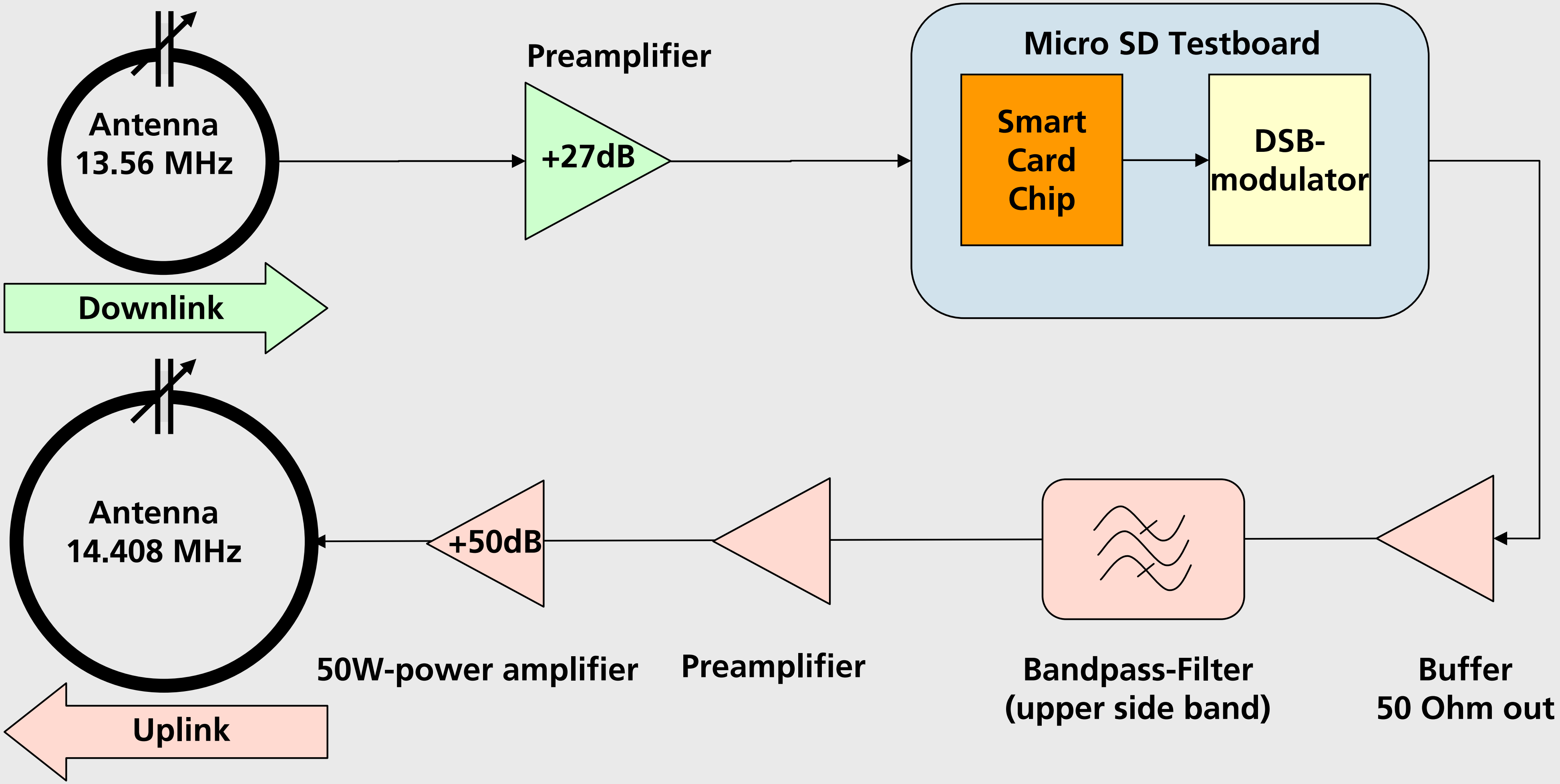
<u>With filtering:</u>

100% of power in the Upper side band!

& smaller bandwidth > higher Q!



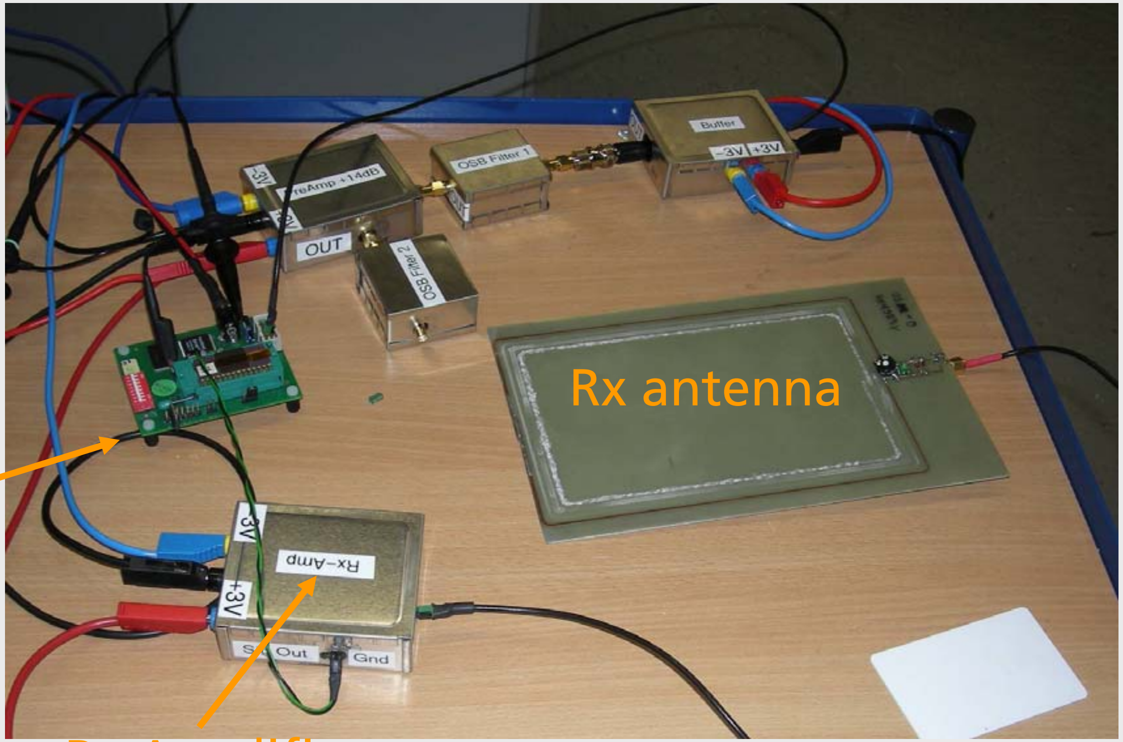
Prototype Implementation



Measurement Setup

Receiver frontend

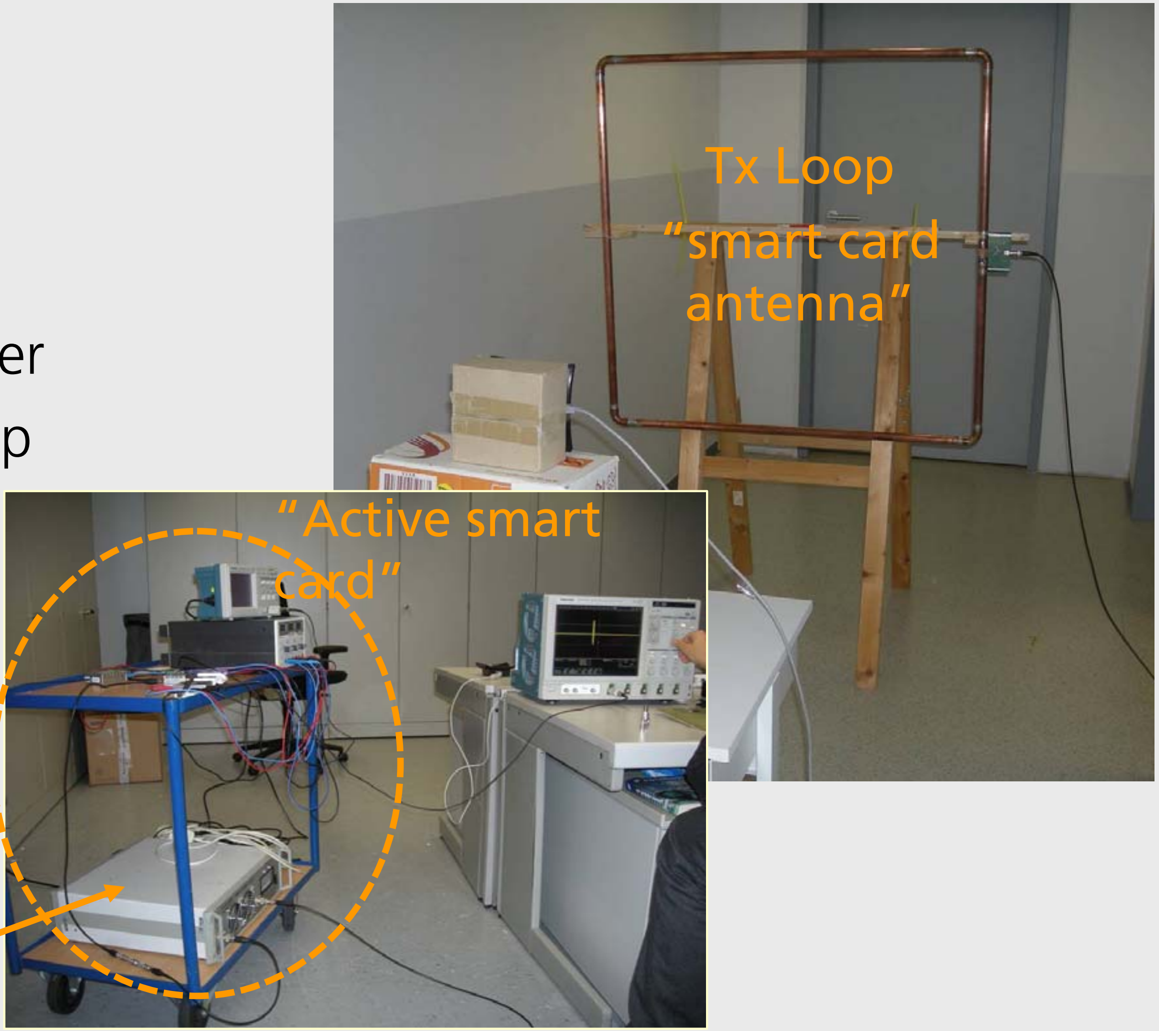
- Rectangular loop antenna 19 x 12.5 cm² (f=13.56MHz / Q = 27)
- Amplifier with 27dB gain



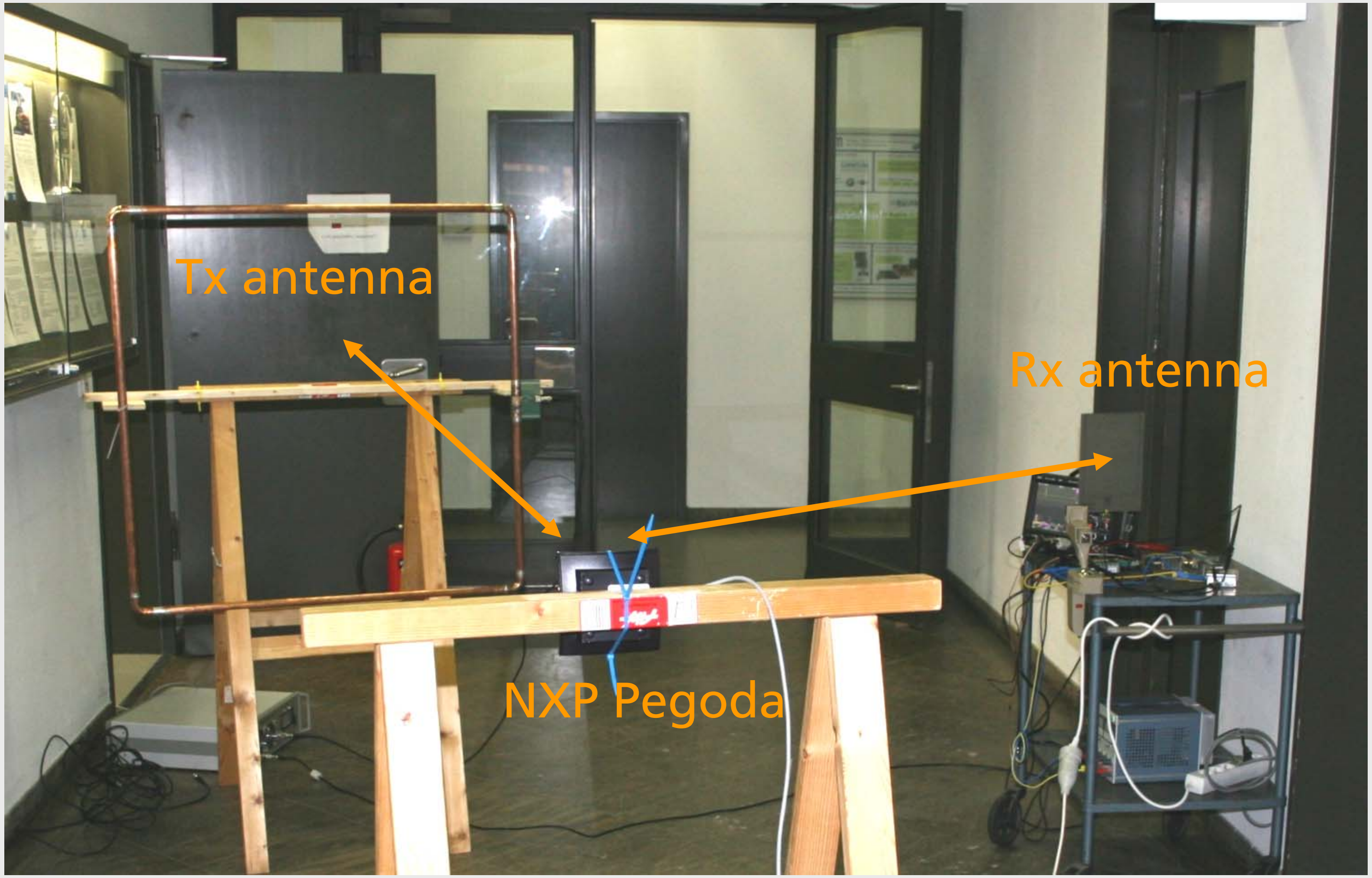
Measurement Setup

Transmitter frontend

- Coupled resonator filter
- Preamplifier
- Commercial 50 Watt amplifier
- Rectangular copper tube loop antenna 1 x 1 m² (f=14.408MHz / Q = 22)



Measurement Setup



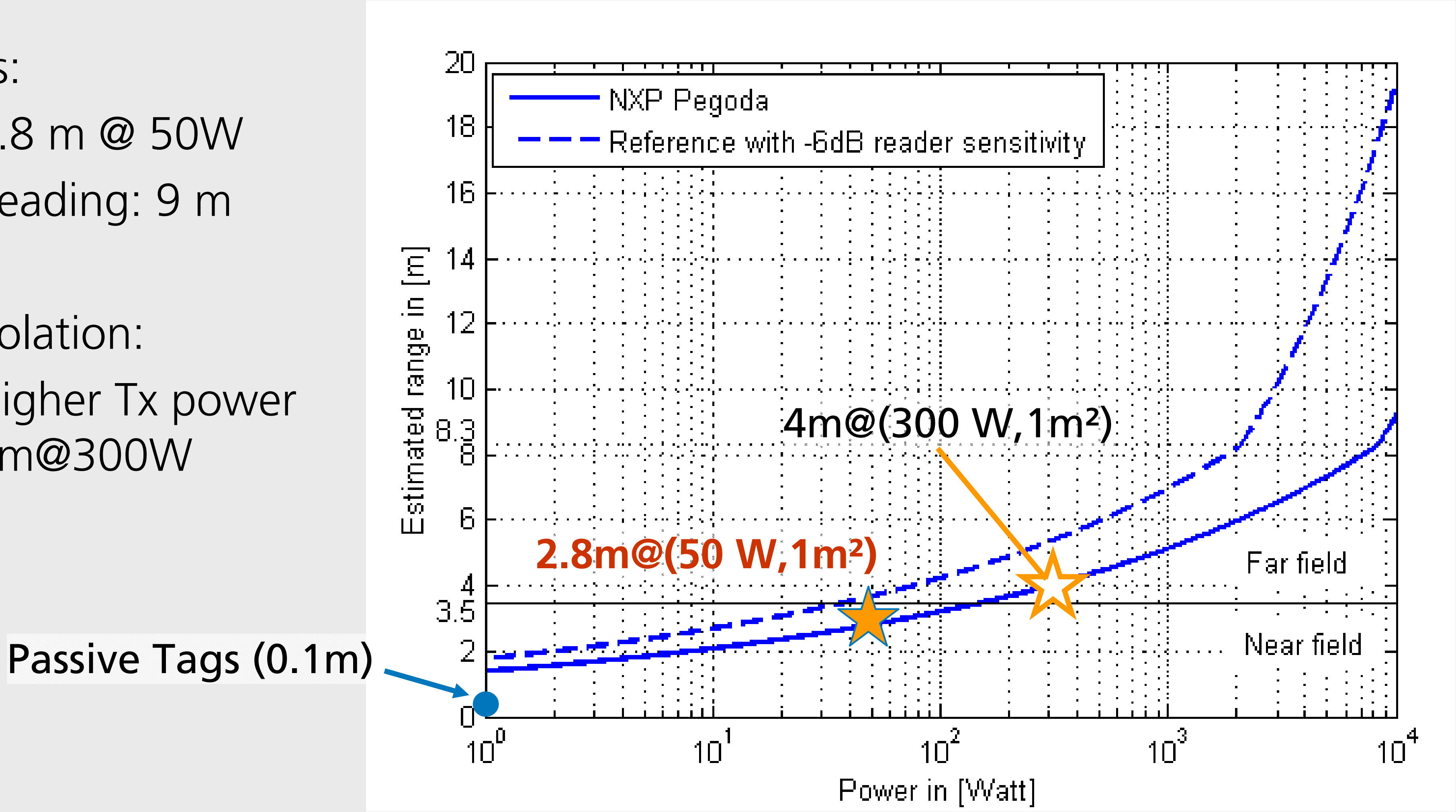
Measurement Results and Extrapolation

Results:

- 2.8 m @ 50W
- Reading: 9 m

Extrapolation:

- Higher Tx power 4m@300W



4m@(300 W,1m²)

2.8m@(50 W,1m²)

Passive Tags (0.1m)

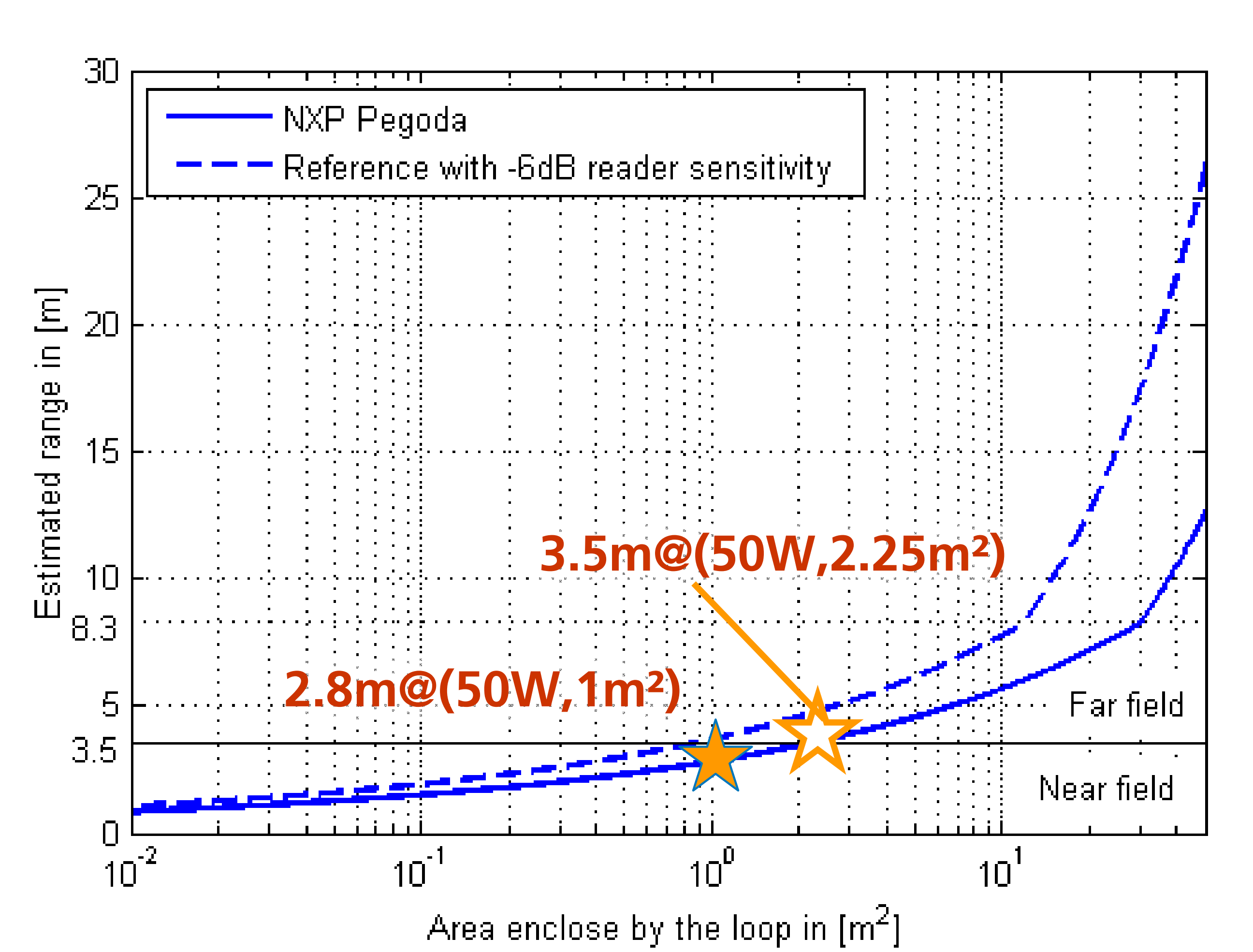
Measurement Results and Extrapolation

Results:

- 2.8 m @ 50W
- Reading: 9 m

Extrapolation:

- Tx power 300W
- & Antenna size 1.5m x 1.5m
- Calculated range 5.5m



3.5m@(50W,2.25m²)

2.8m@(50W,1m²)

Conclusion

Limiting factors of Rx range :

- Signal-to-noise ratio (SNR) / man made noise
- Without any other readers close by we achieved a reading range of 9m
- With other readers: CW signal / signal interference ➔ additional filtering

Limiting factors of Rx range :

- With a 1x1m² antenna and a 50 Watt amplifier we achieved a range of 2.8m
- High Rx power and huge antennas quickly ending up with equipment like a "broadcast radio station"

An attack over several meters is difficult to install (no handy briefcase) and therefore limited to very few selected places