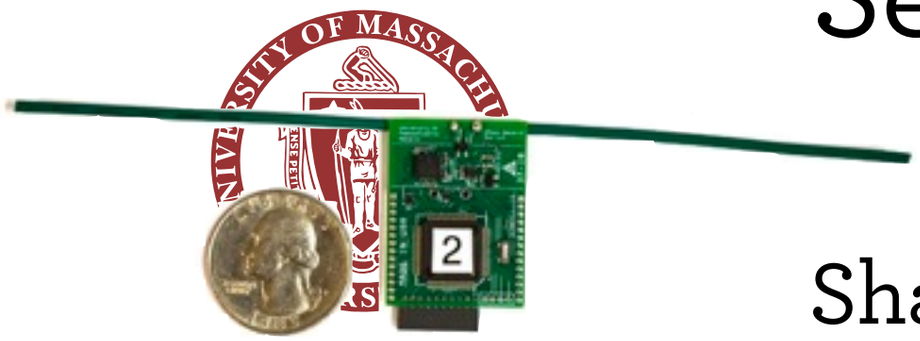
RFIDsec 11

Hands-on Programming of Batteryless, RFID-Scale Computers with Sensors



Shane S. Clark, Benjamin Ransford,
Negin Salajegheh, and Hong Zhang

RFIDsec 11

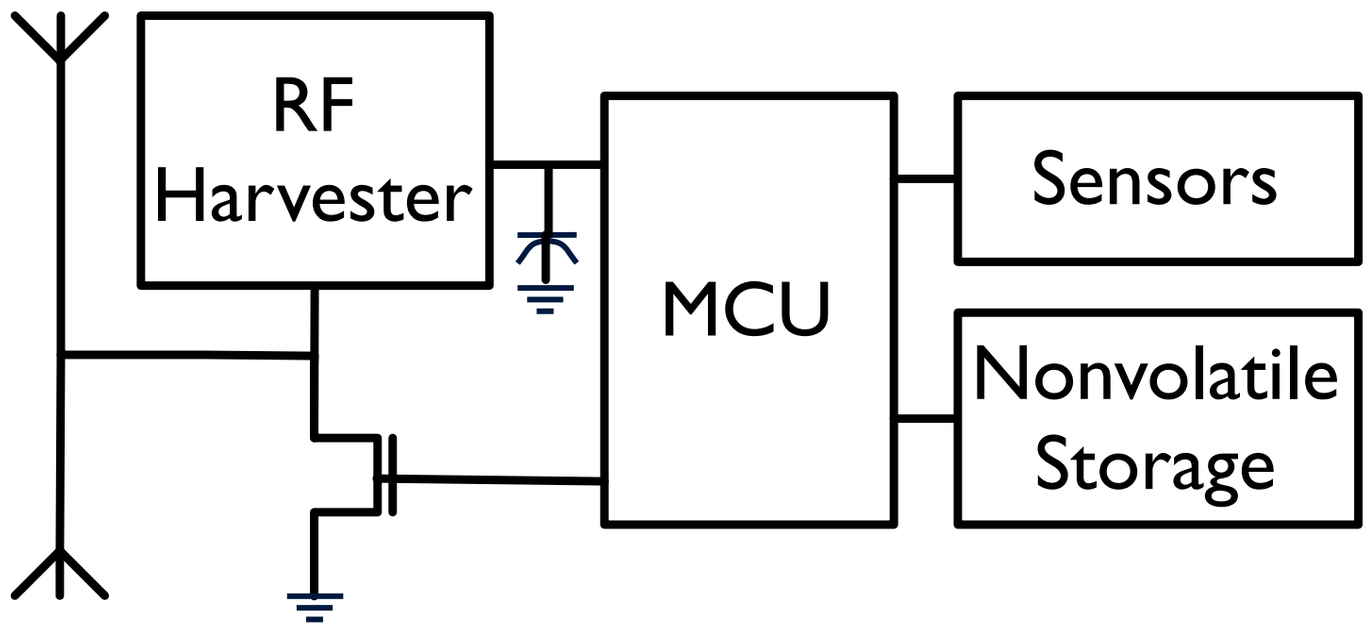
RFIDsec 2011
Sunday, June 26, 2011

Outline

- Definitions & Background
- 10:30am — Coffee Break
- Intro to the Moo & Toolchain
- 12:30pm — Lunch
- Guided Programming & Debugging
- 3:30pm — Coffee Break
- Unguided Programming

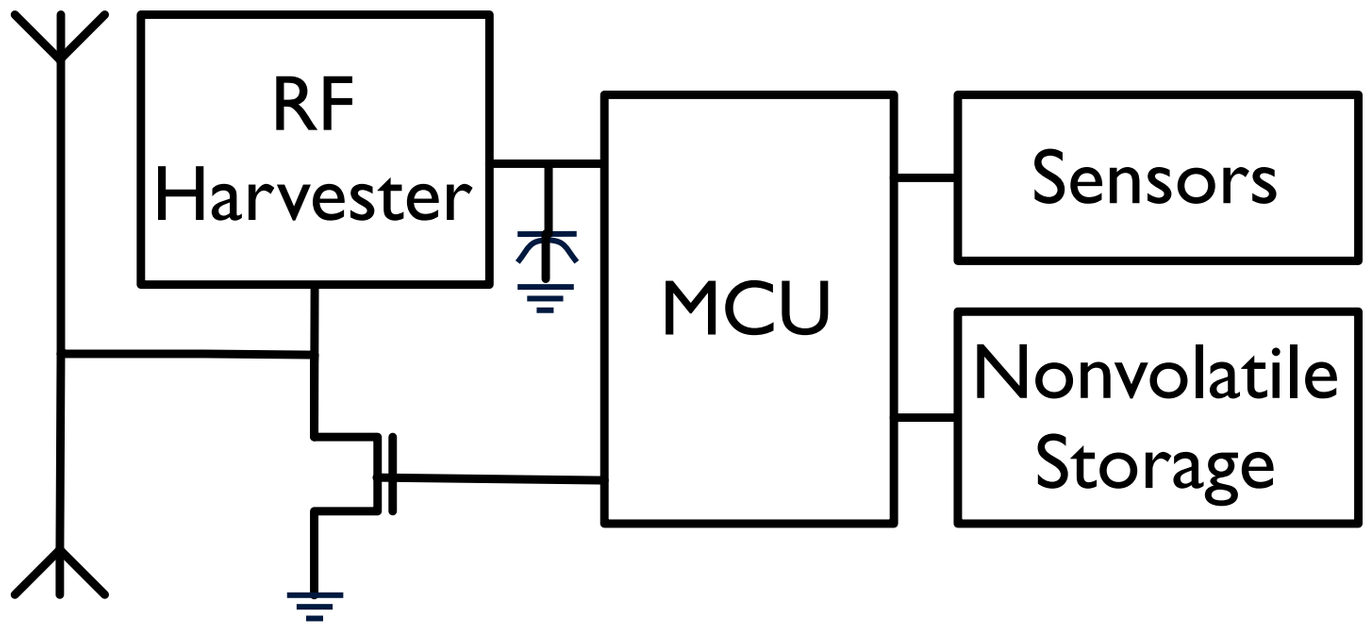
RFID-Scale Devices

[Impinj®, Inc.]



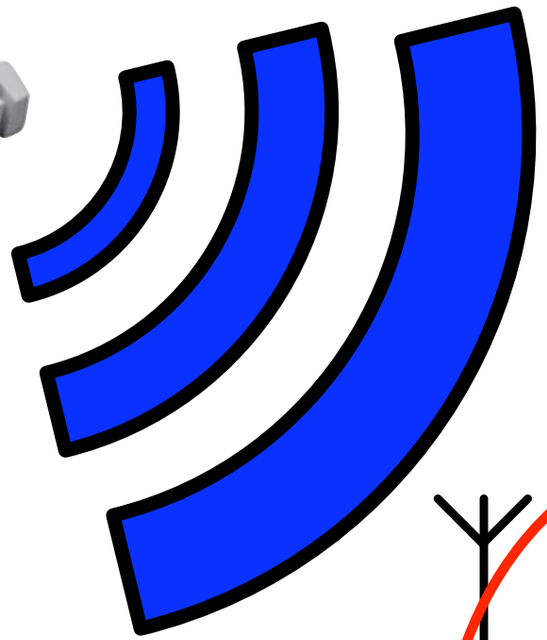
RFID-Scale Devices

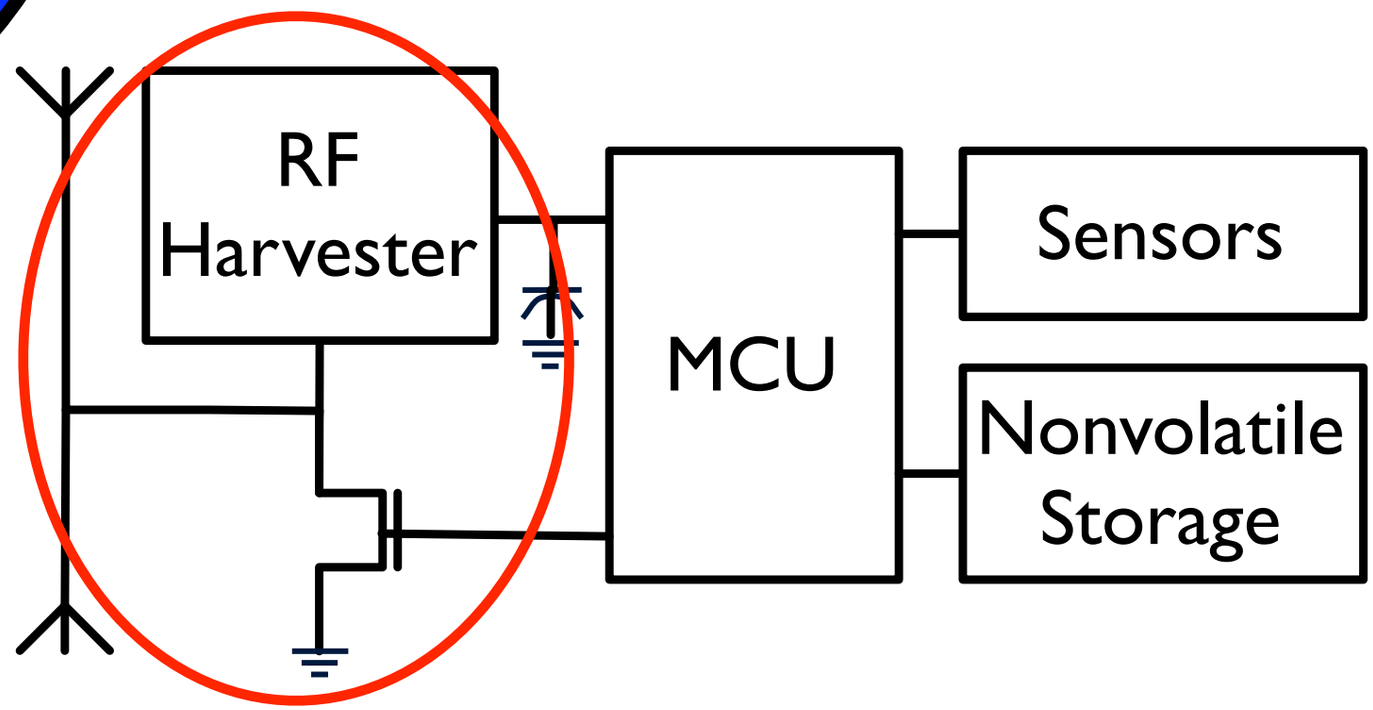
[Impinj®, Inc.]



RFID-Scale Devices

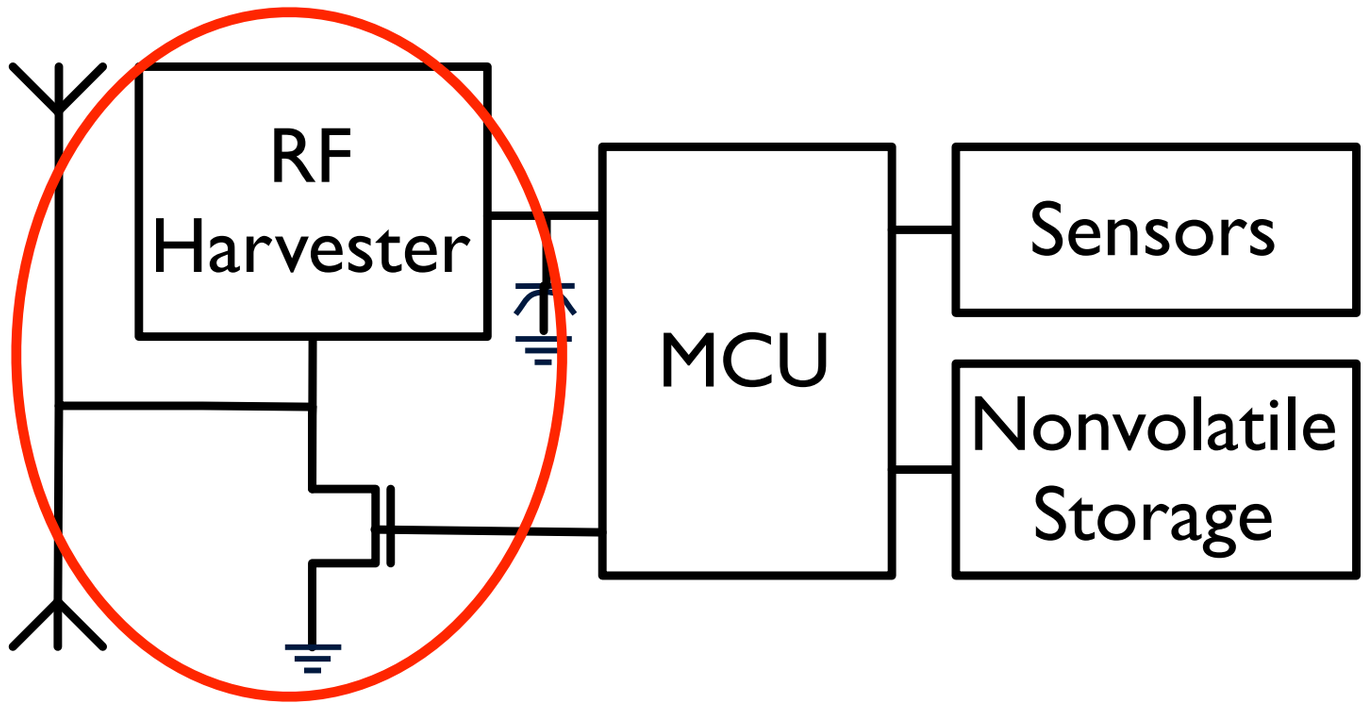
[Impinj®, Inc.]





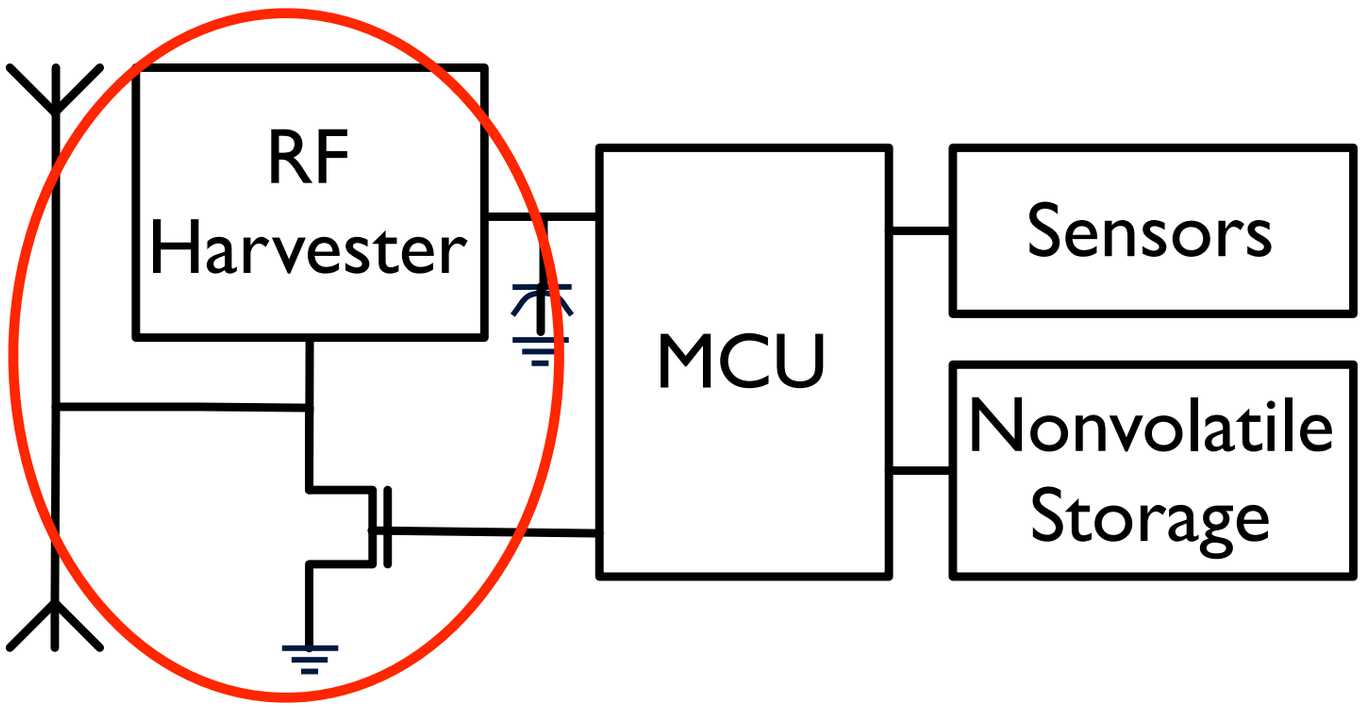
RFID-Scale Devices

[Impinj®, Inc.]



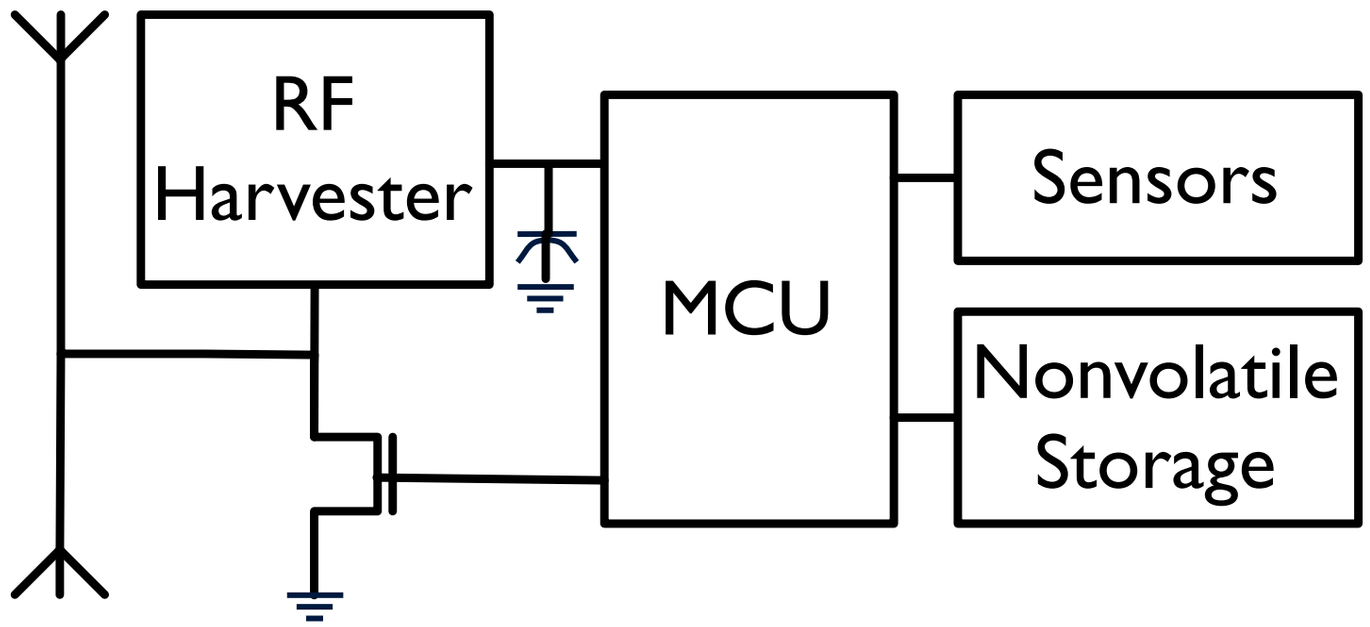
RFID-Scale Devices

[Impinj®, Inc.]



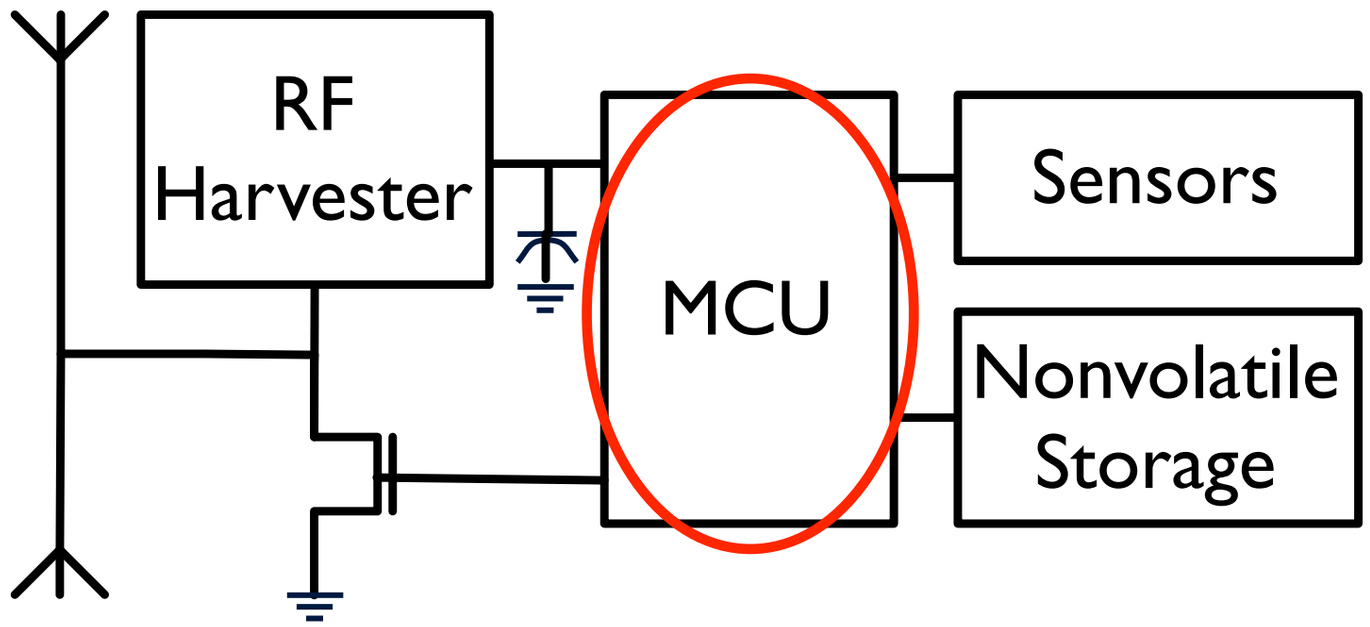
RFID-Scale Devices

[Impinj®, Inc.]



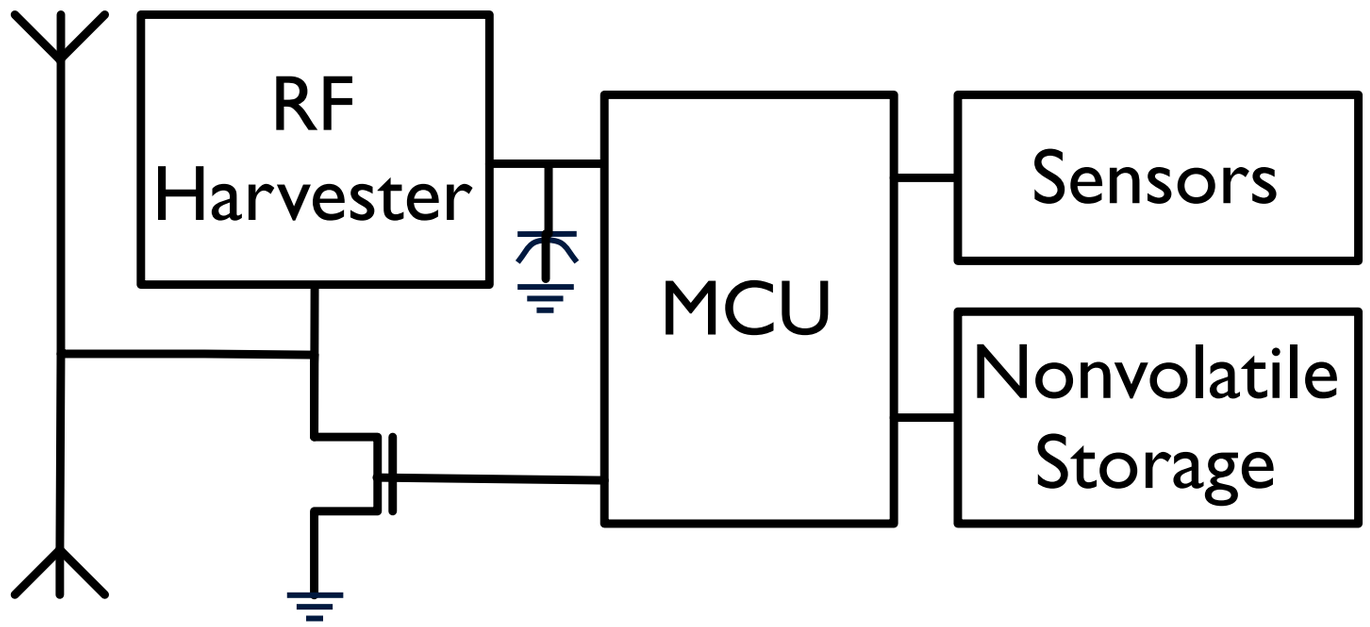
RFID-Scale Devices

[Impinj®, Inc.]



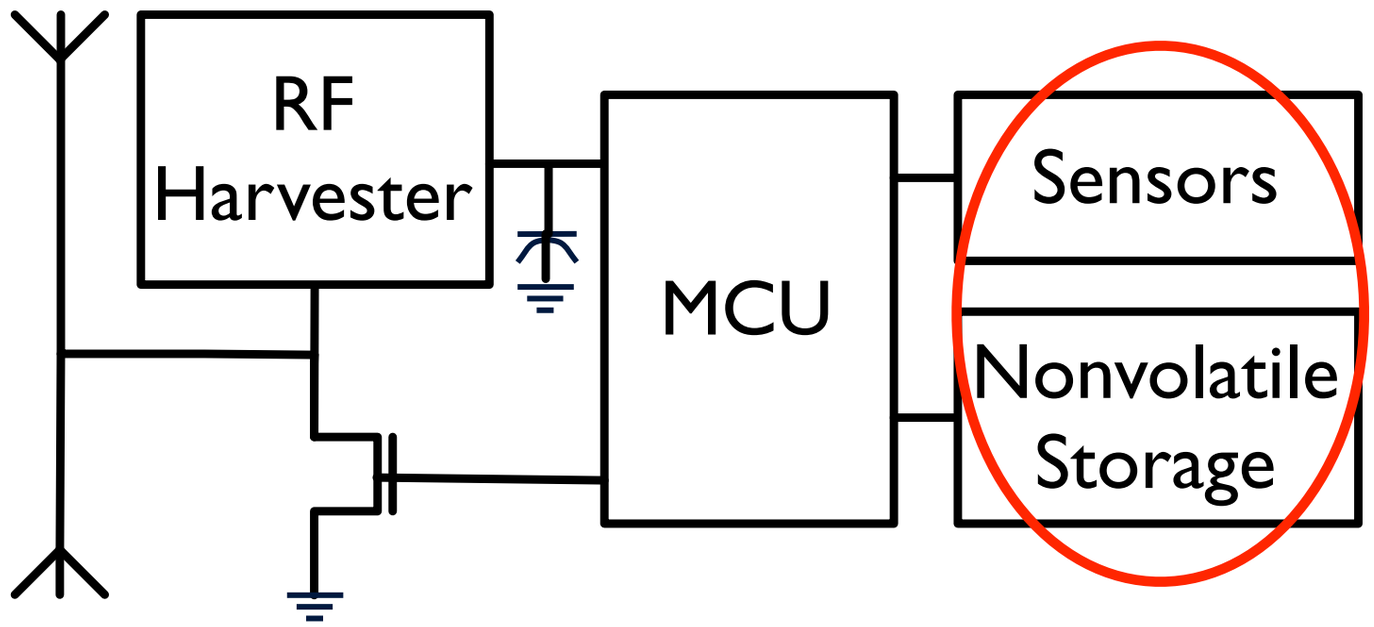
RFID-Scale Devices

[Impinj®, Inc.]



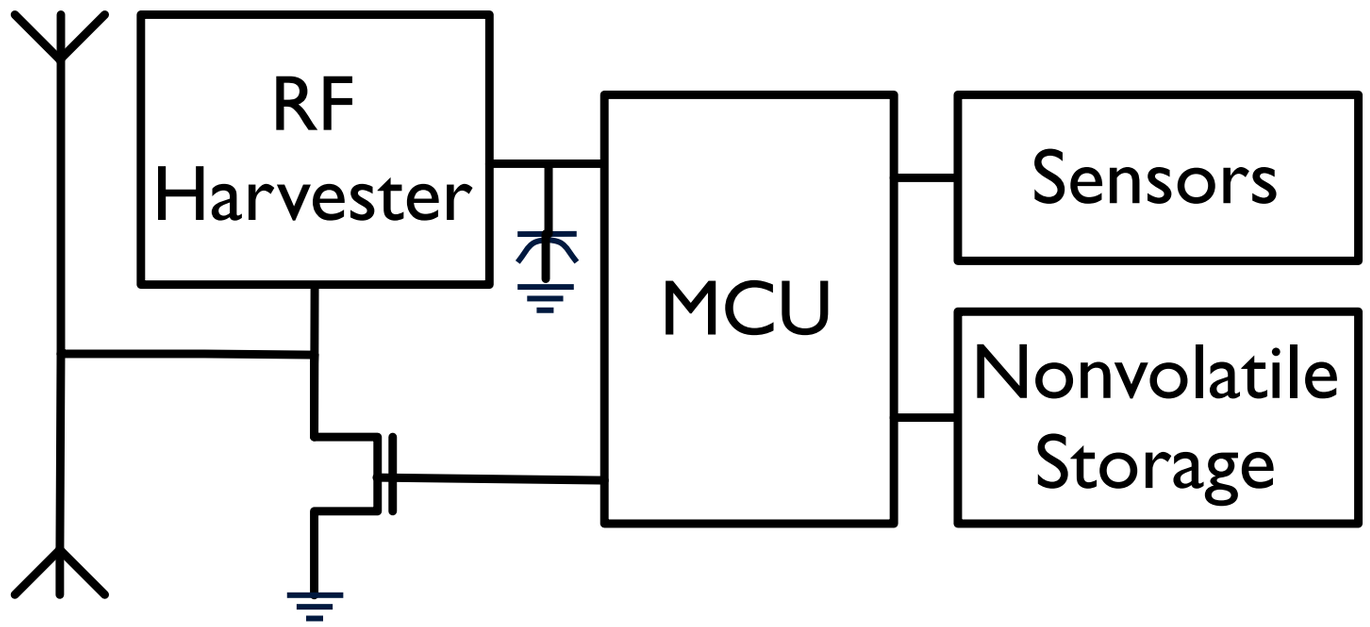
RFID-Scale Devices

[Impinj®, Inc.]



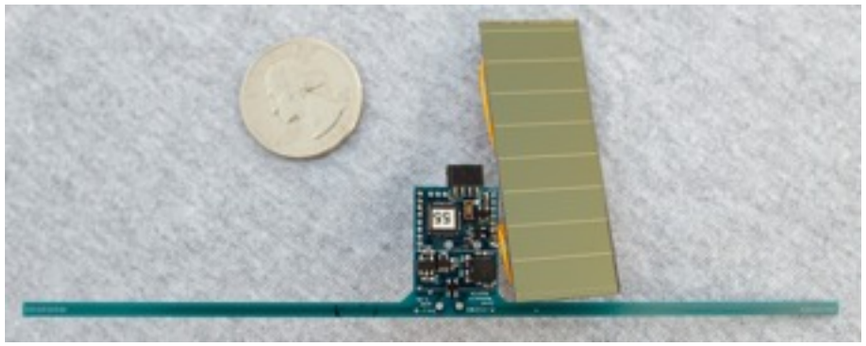
RFID-Scale Devices

[Impinj®, Inc.]



Energy Harvesting

- Other sources are possible
  - Solar
  - Vibration
  - Thermal differentials



Readers

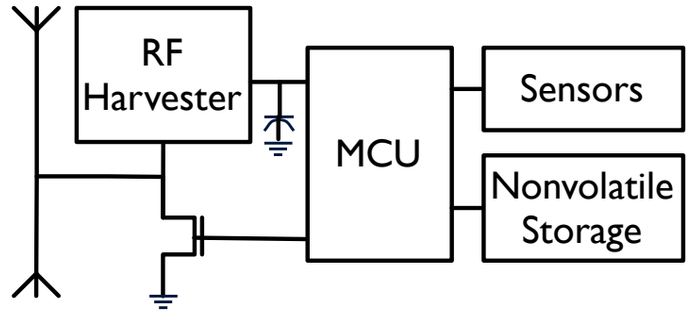
- The Moo works with (at least) four UHF readers:
  - ThingMagic M5
  - ThingMagic M5e
  - Impinj Speedway
  - GNU Radio + USRP https://www.cgran.org/wiki/Gen2

Communications

- Readers power tags and send messages according to the EPCGlobal Class 1 Generation 2 (C1G2) standard.
- Tags respond to readers via backscatter

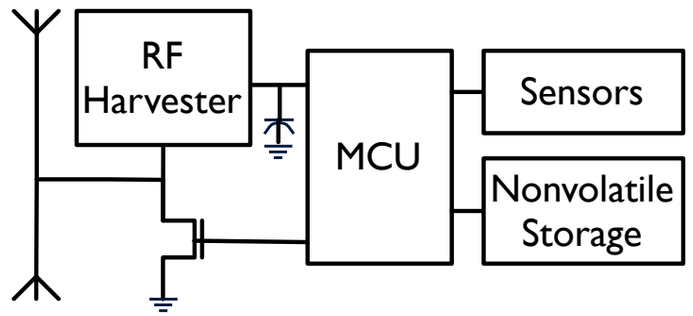
Backscatter

[Impinj®, Inc.]



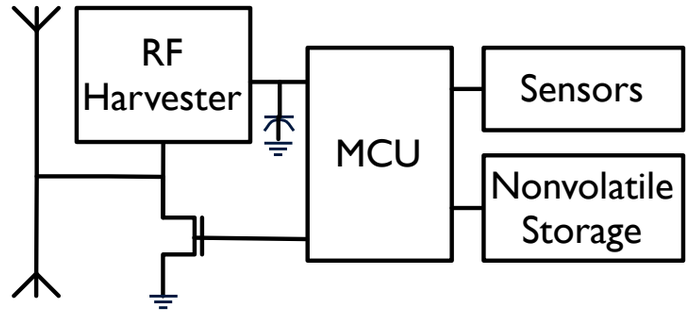
Backscatter

[Impinj®, Inc.]



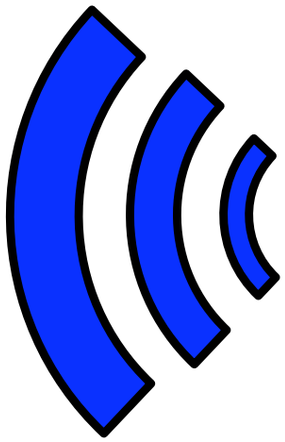
Backscatter

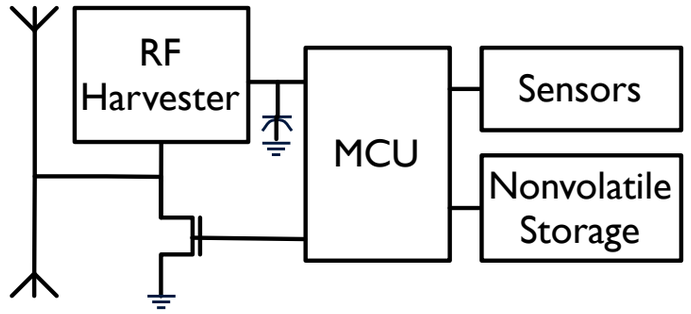
[Impinj®, Inc.]



Backscatter

[Impinj®, Inc.]





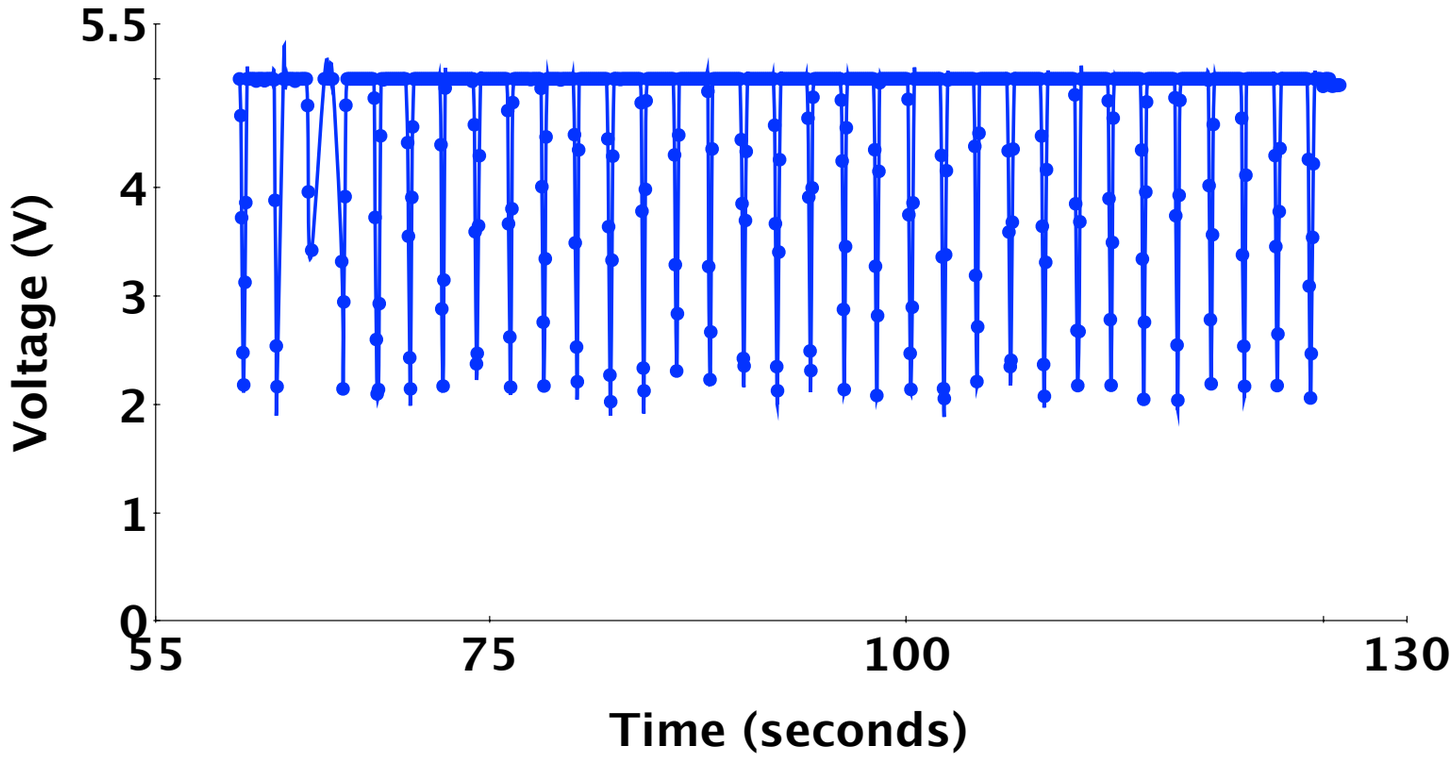
Communications

- Backscatter only requires the tag to switch a single transistor.
  - Communication is very energy-efficient.
  - Tags cannot communicate with one another.

C1G2

- Designed for applications like warehousing/inventory tracking
- Readers *select* and subsequently *query, read,* or *write* tags.

Energy Availability



Energy

- How to gauge harvesting/stored energy
  - Voltage supervisor
    - Interrupt-driven threshold detection
  - ADCs
    - Polling-based exact measurement

Energy

- Hardware mechanisms for coping
  - Other harvesters
  - Larger caps
    - Longer running times → longer charging times
    - See Gummeson et al., Mobisys '10

RFIDsec 11

Applications (a literature review)

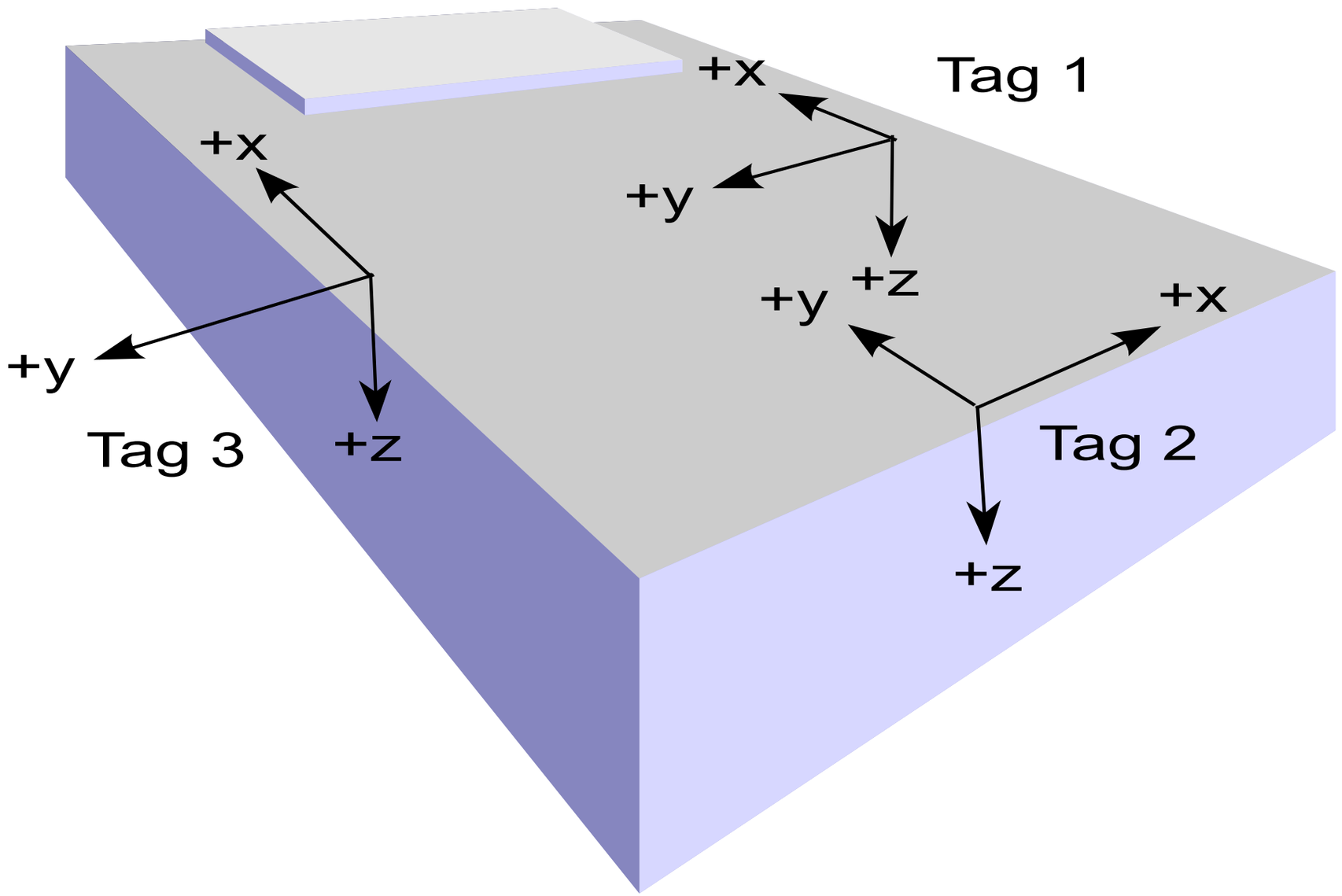
All of the following papers can be found on the WISP wiki publication page:

http://www.wisp.wikispaces.com/publications

Activity Recognition

Buettner et al., Ubicomp '09

Sleep Monitoring



Hoque et al., Wireless Health ’10

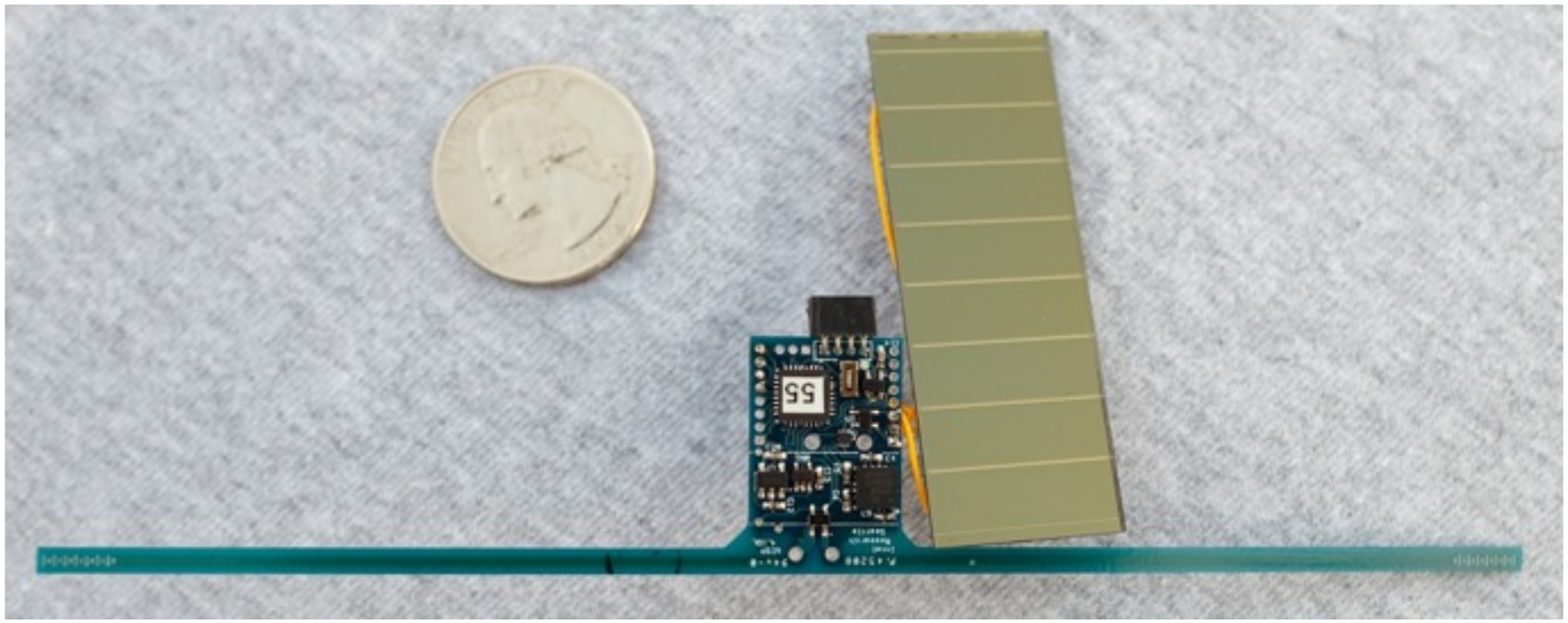
Motion-Based Access Control

Czeskis et al., CCS '09
Saxena and Voris, RFIDSec '10

Random Number Generation

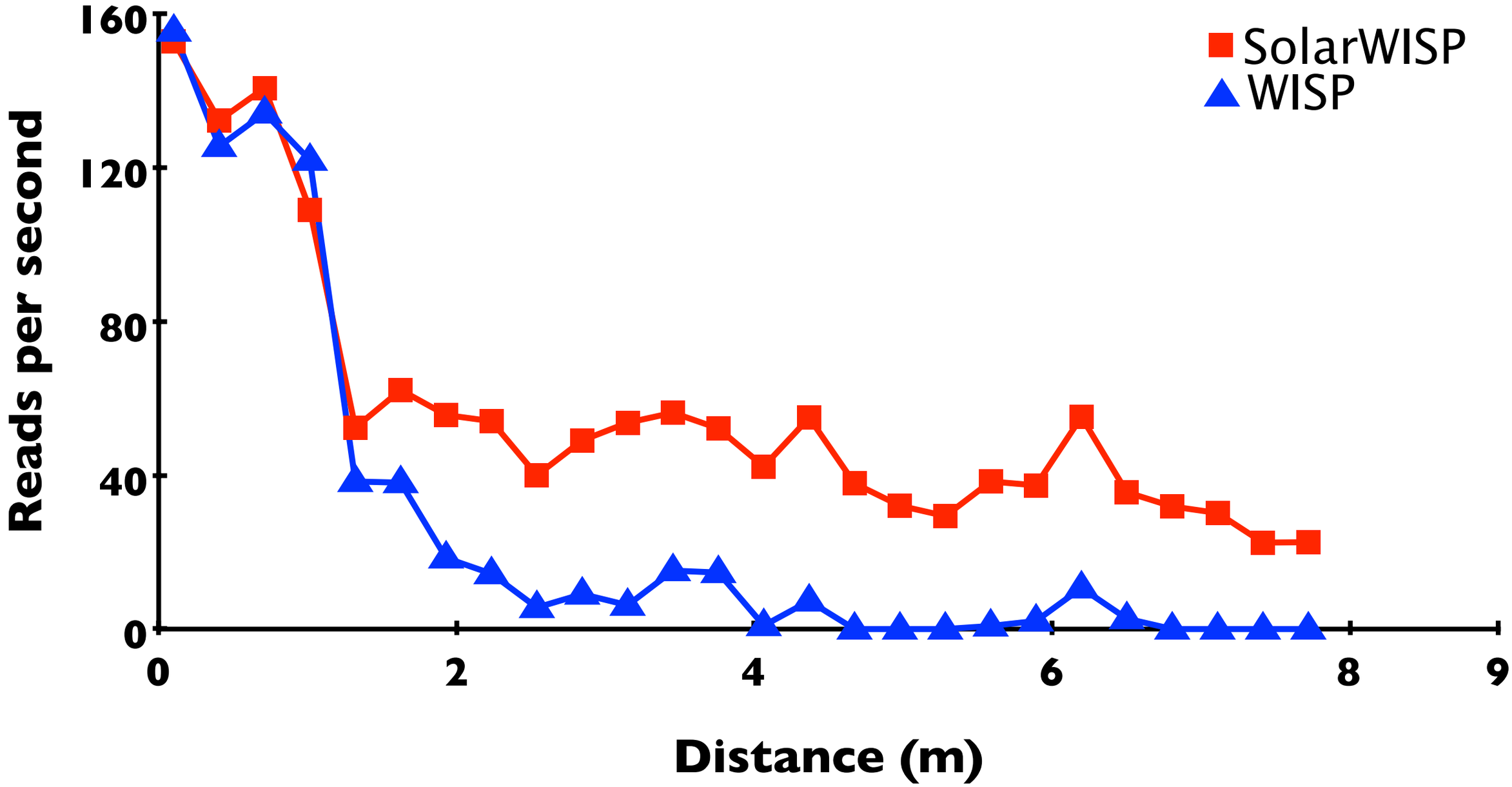
- Accelerometers as PRNGs
- Voris el al., WiSec ’11

SolarWISP

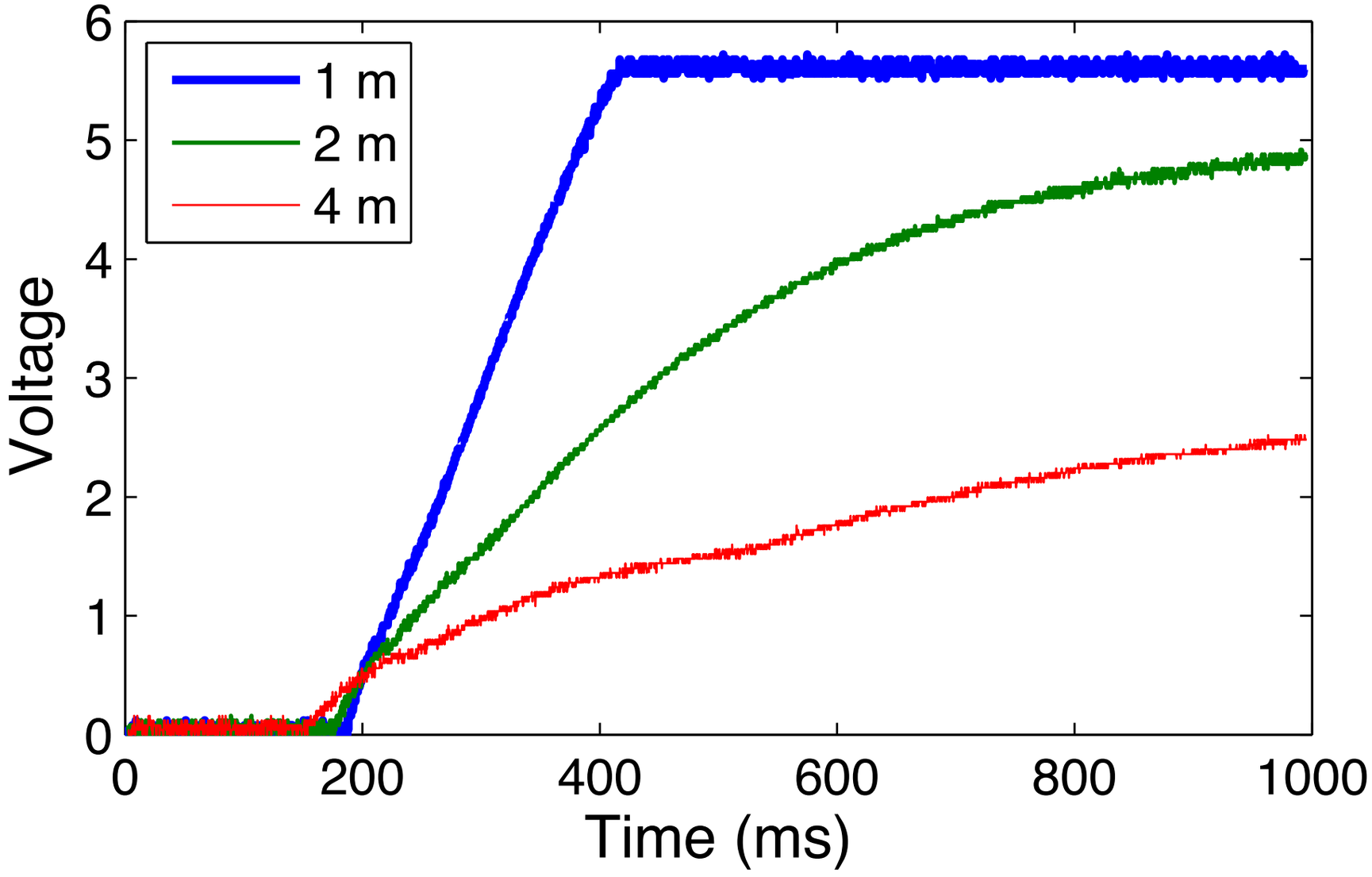


Clark et al., Hotpower ’09, Gummeson et al., Mobisys ’10, Sample et al., RFID ’11

Read Range Benefits

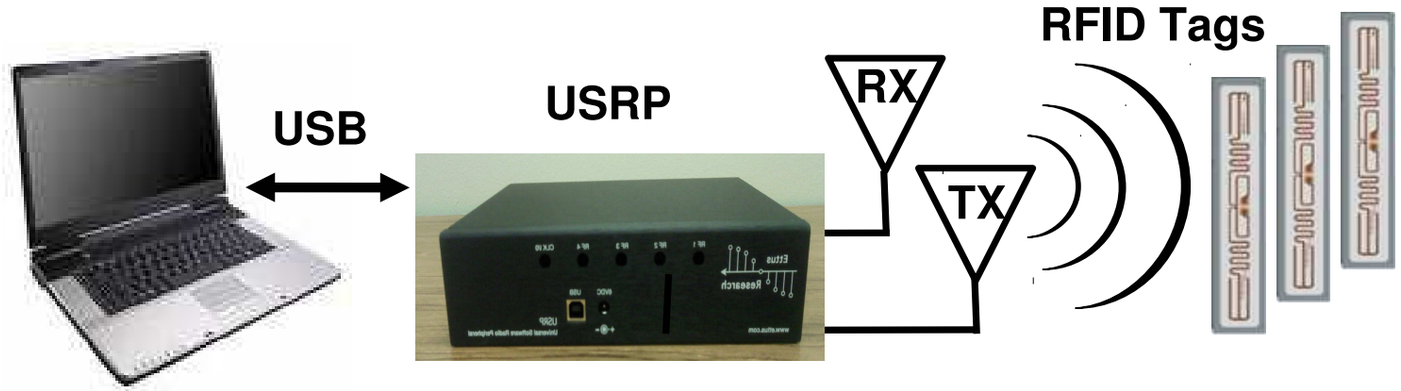


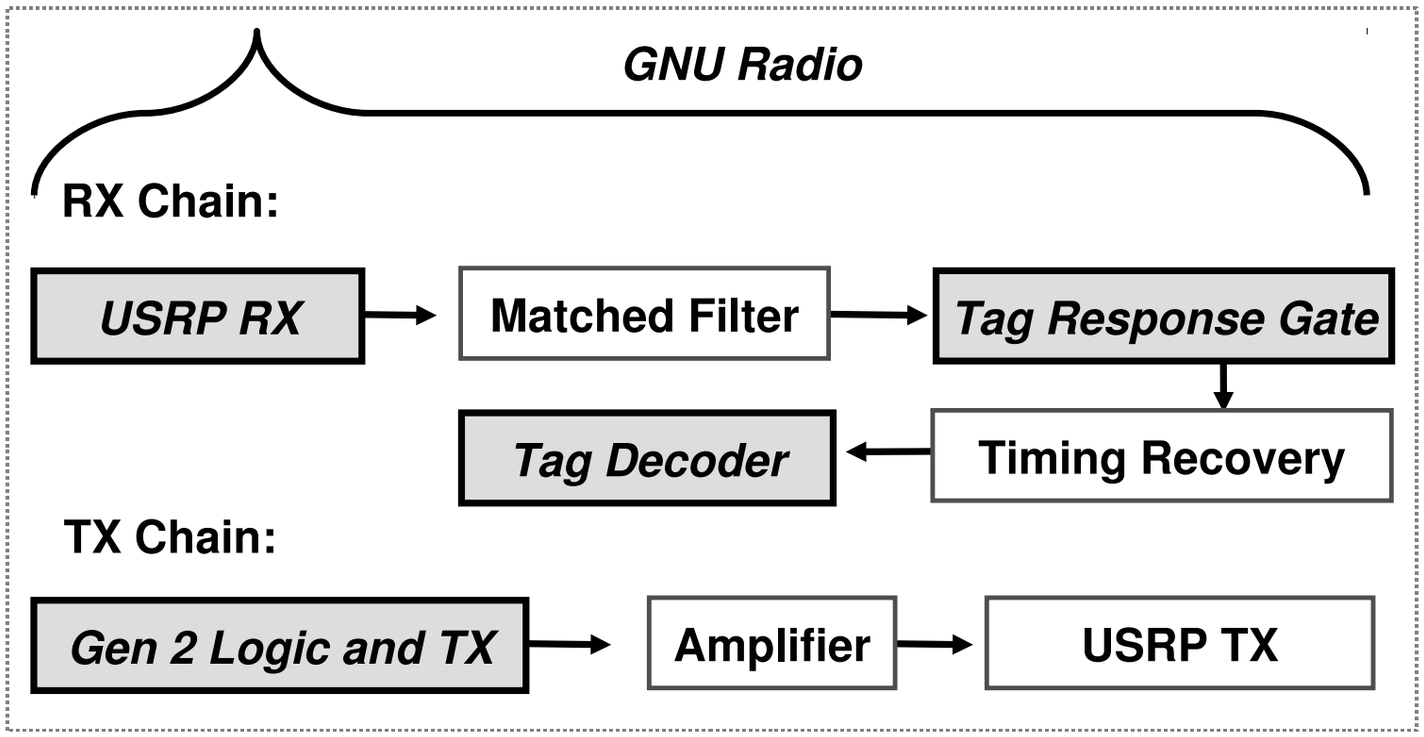
Dewdrop



Buettner et al., NSDI '11

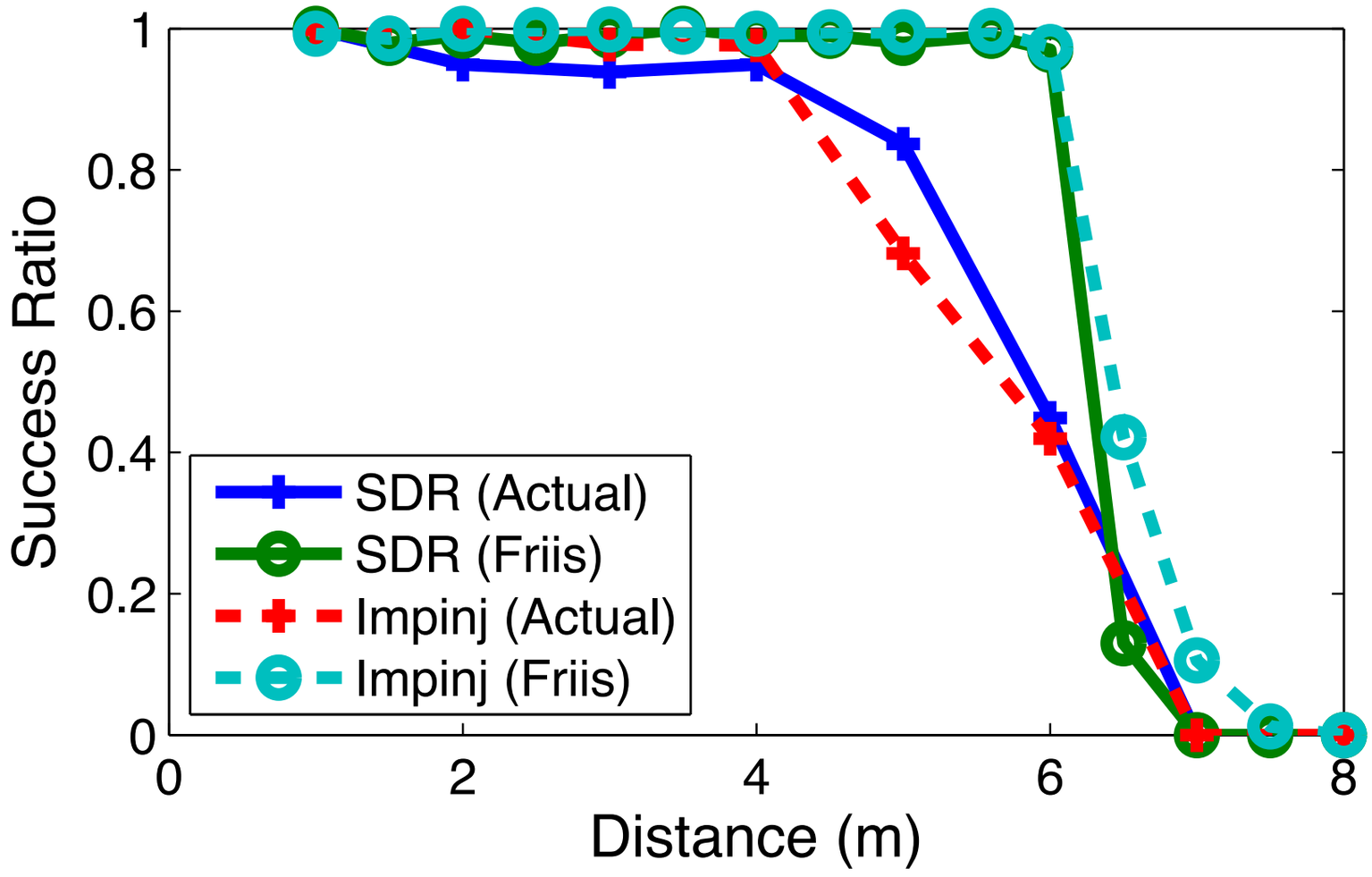
USRP Reader





Buettner, techreport '11

USRP Performance



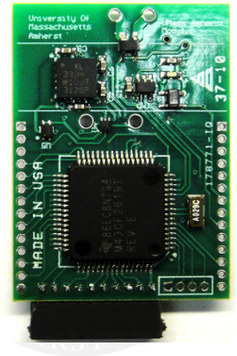
Yeager et al., IEEE Journal of Solid State Circuits ’10

RFIDsec 11

Coffee Break

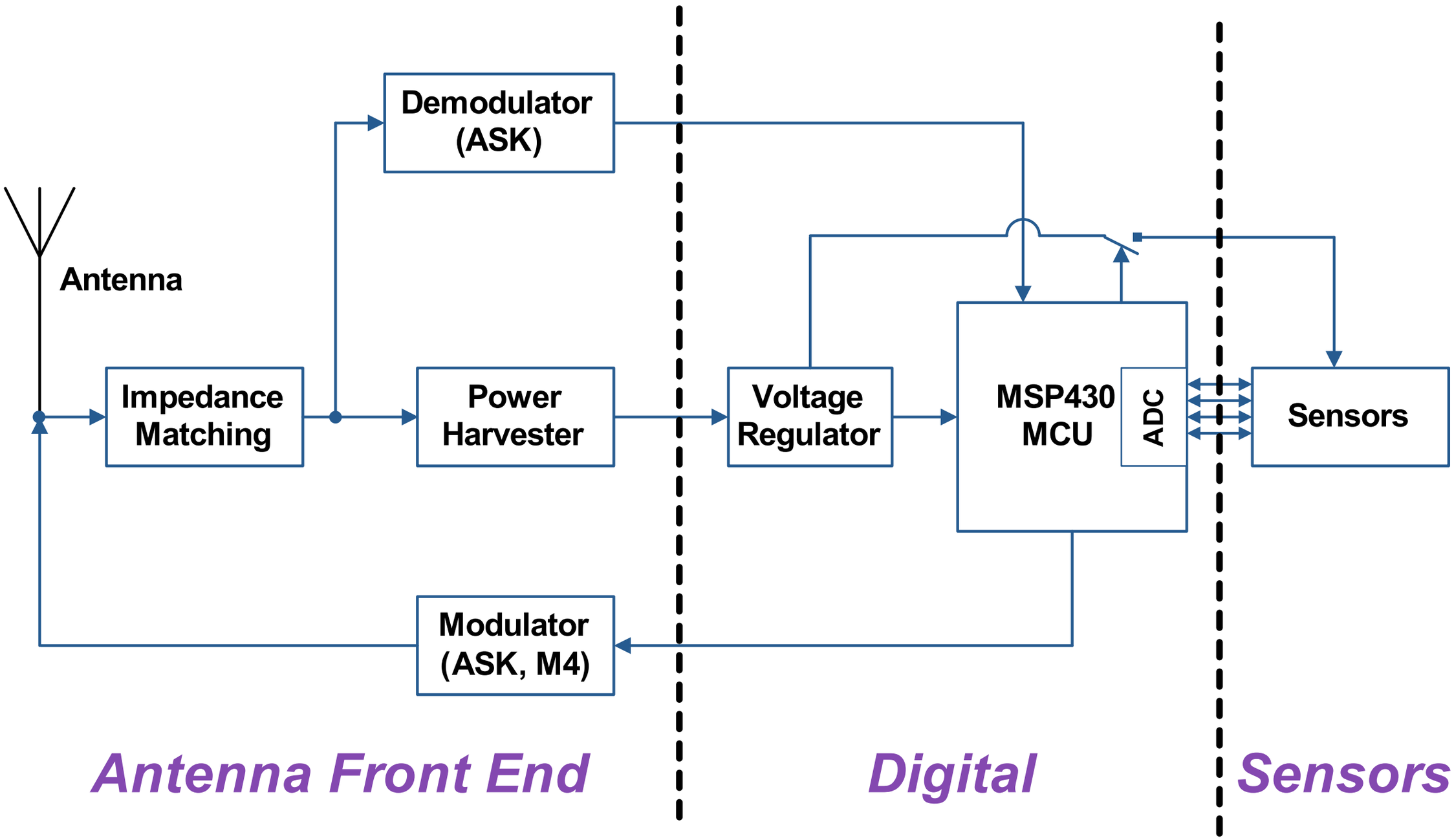
The Moo

- Details of the Moo itself
  - Hardware specs
  - Design decisions



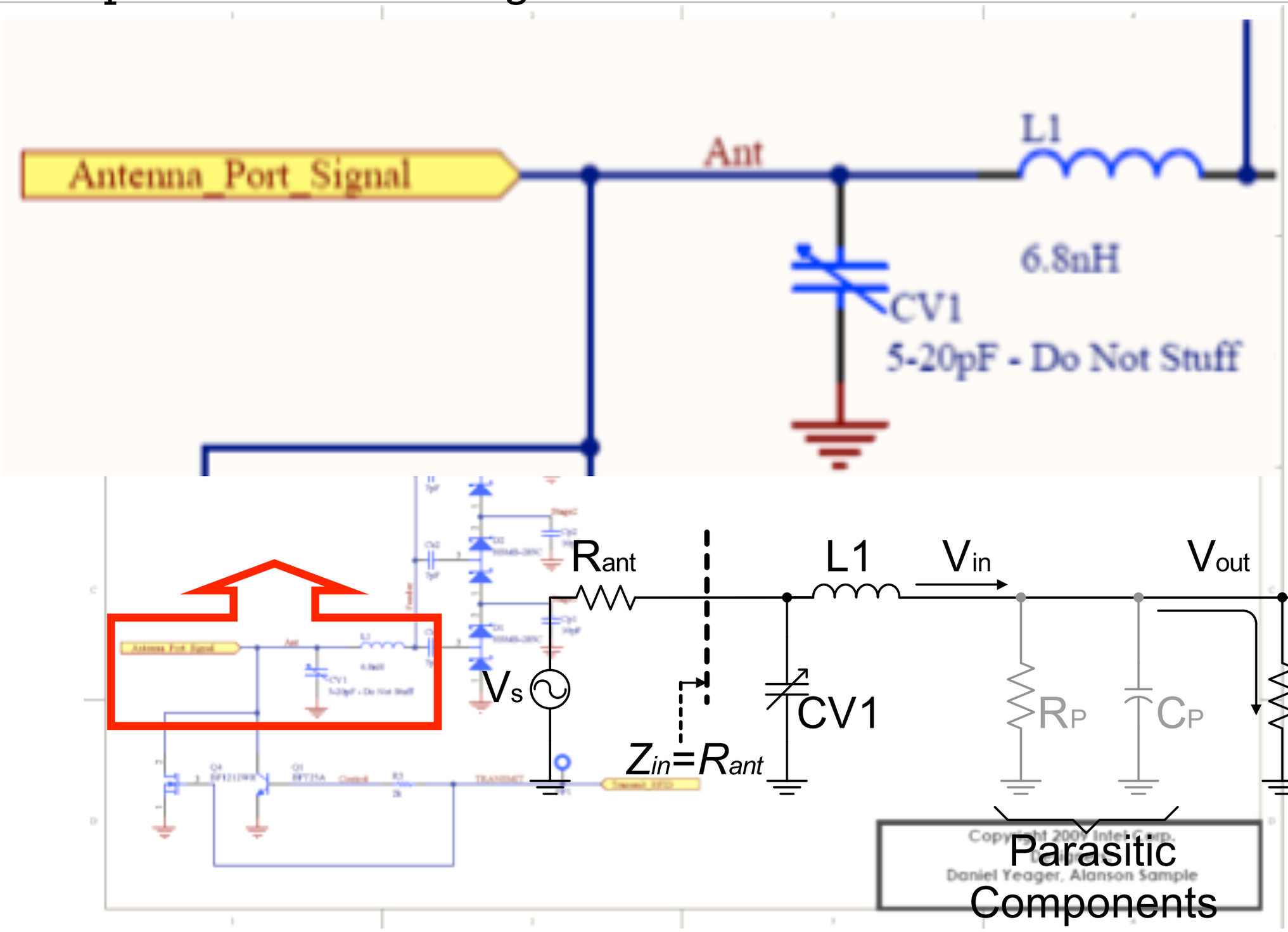
1. How does Moo 1.1 work?

- Block Diagram



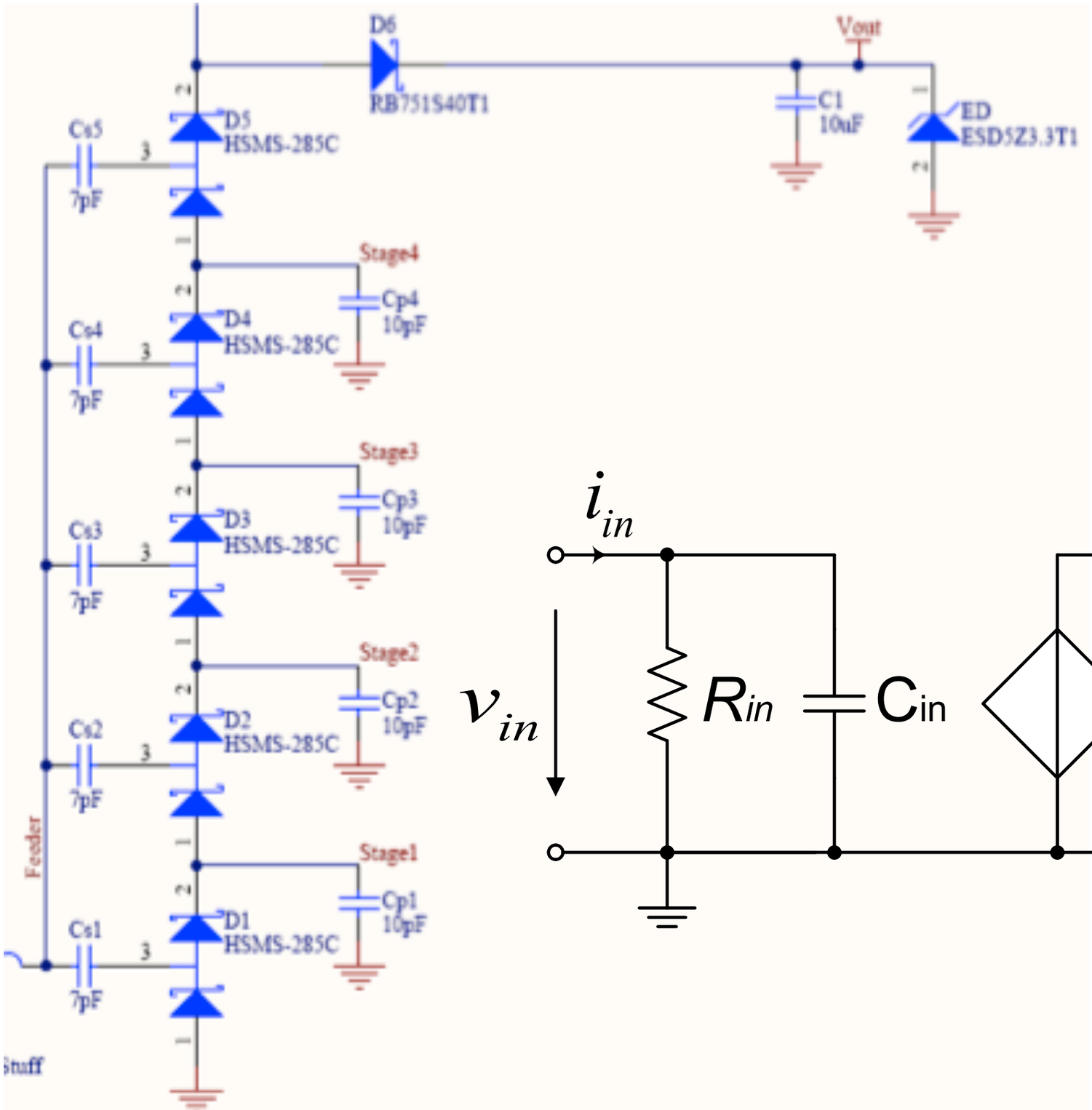
1. How does Moo 1.1 work?

- Impedance Matching



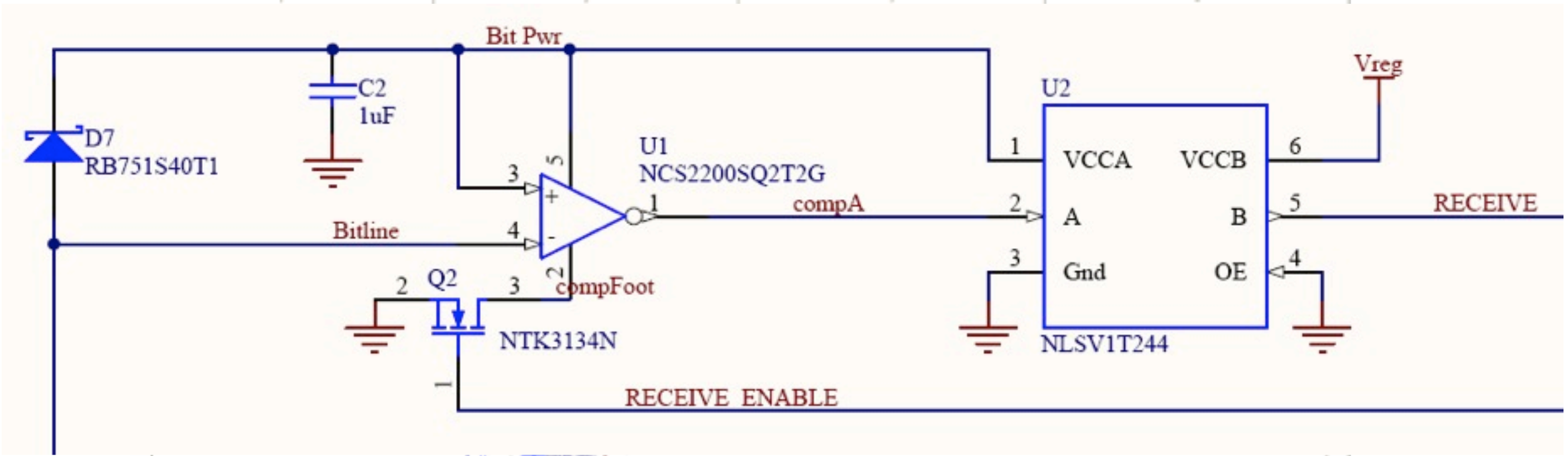
1. How does Moo 1.1 work?

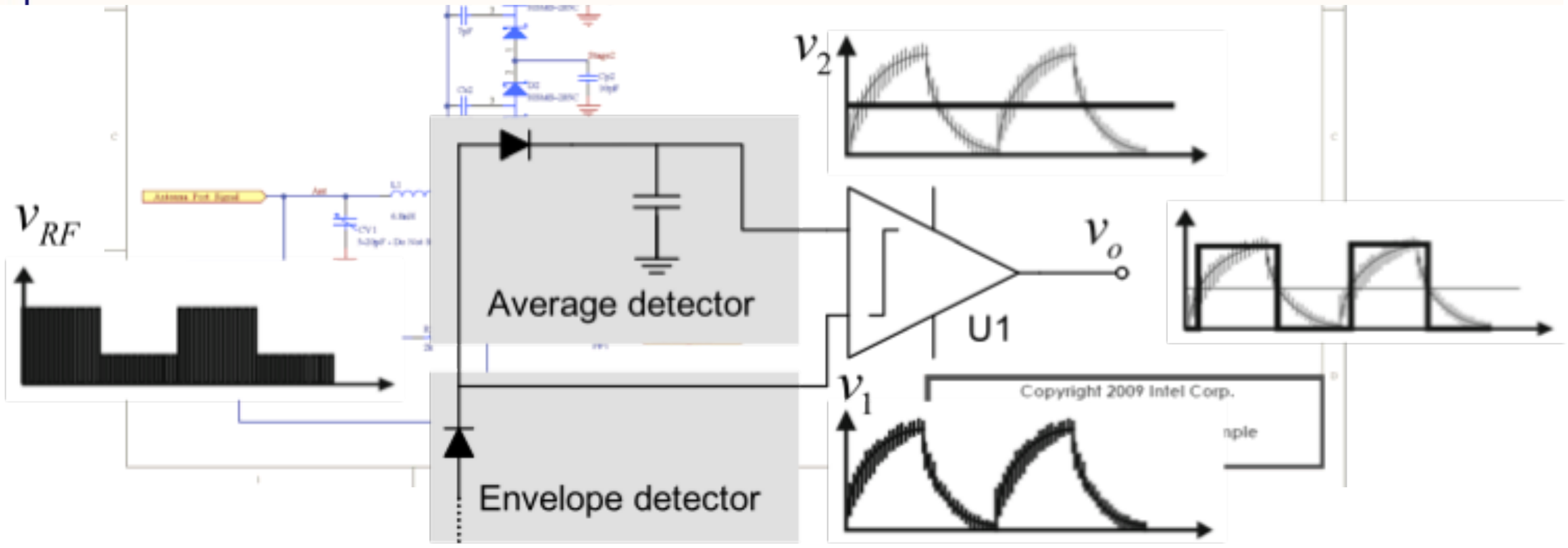
- Power Harvester



1. How does Moo 1.1 work?

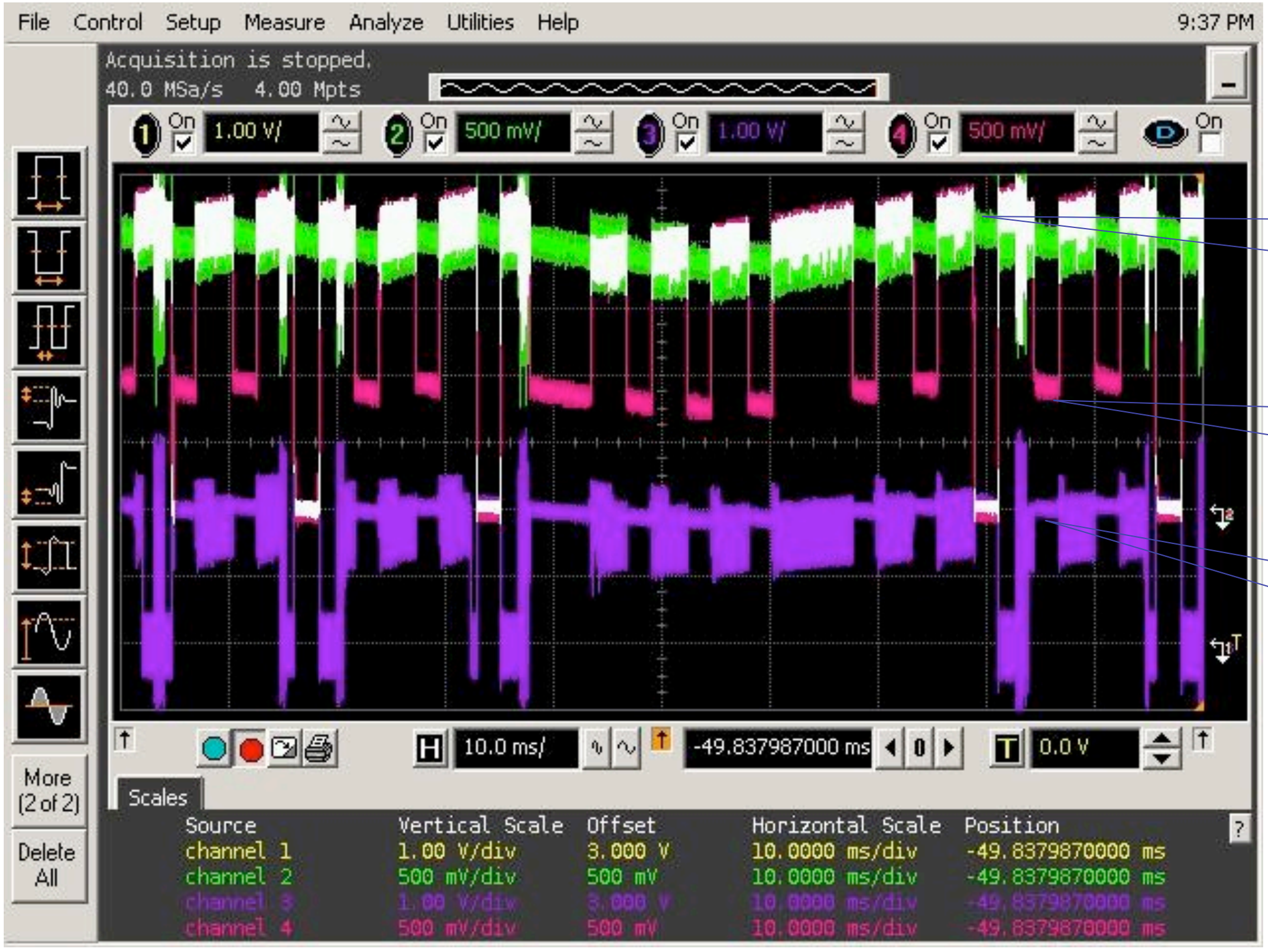
- Demodulator (ASK – Amplitude-Shift Keying)





1. How does Moo 1.1 work?

- Demodulator (ASK – Amplitude-Shift Keying)



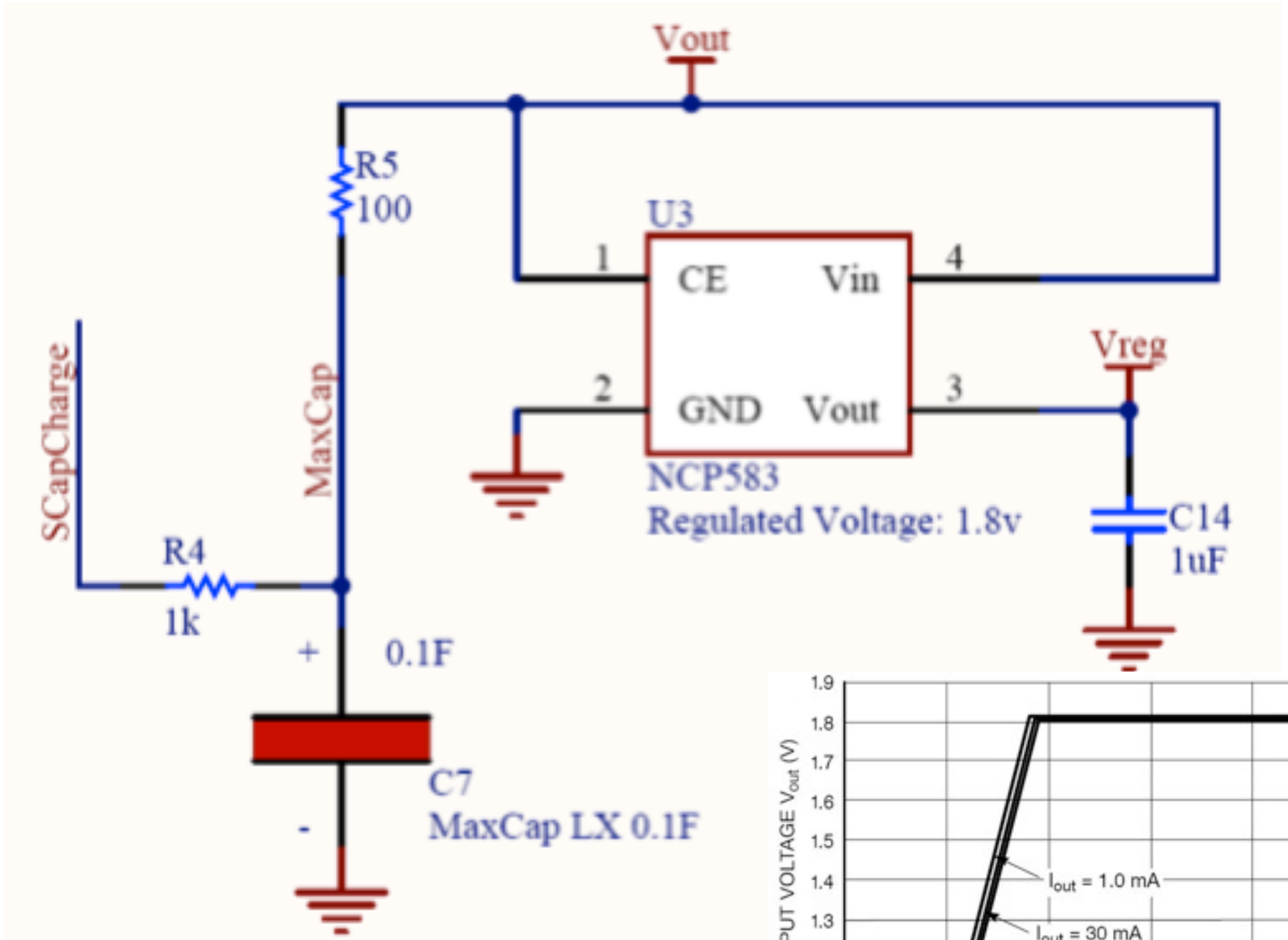
Green: Bit Power

Pink: Bit Line

Purple: CompA

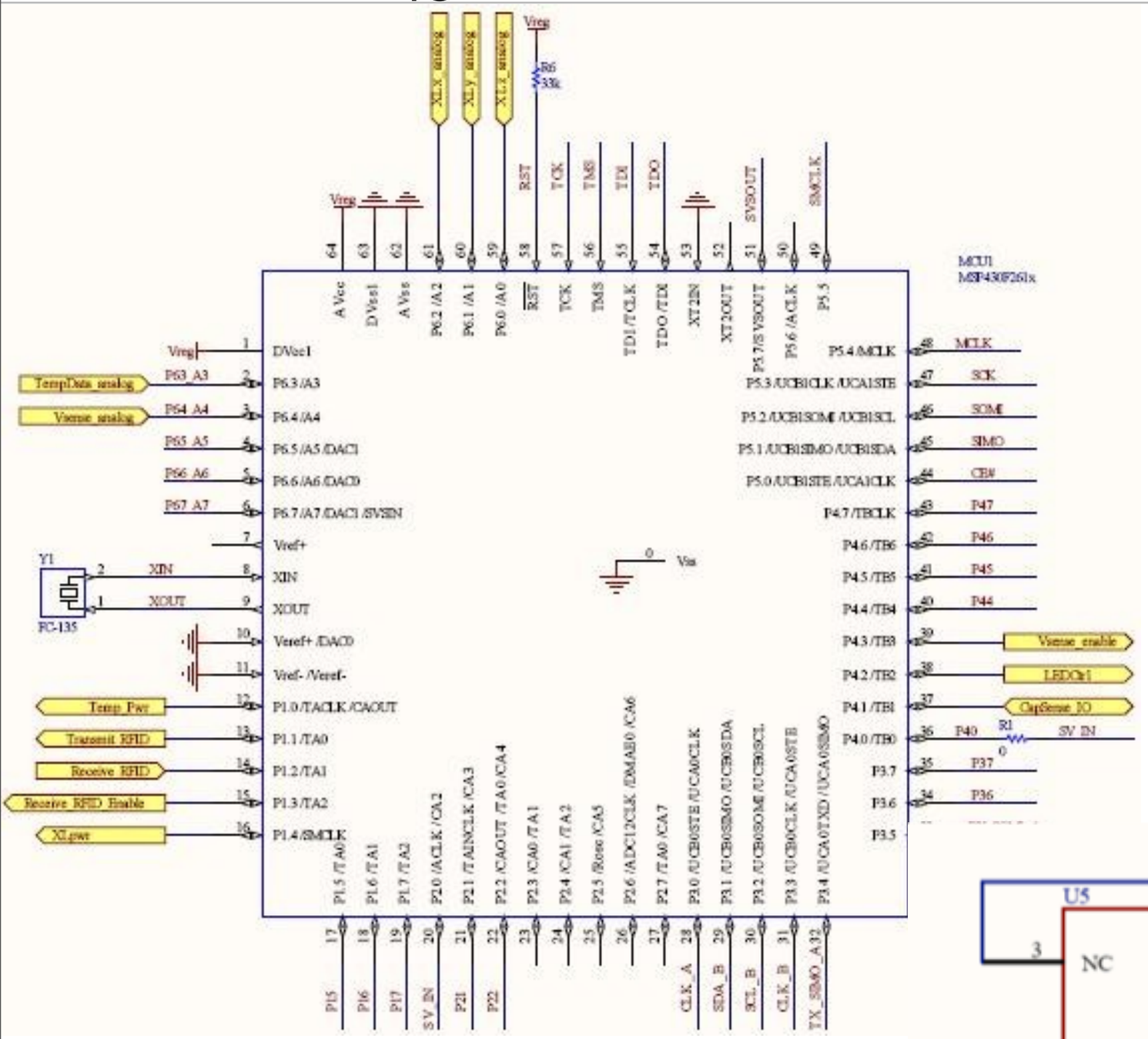
1. How does Moo 1.1 work?

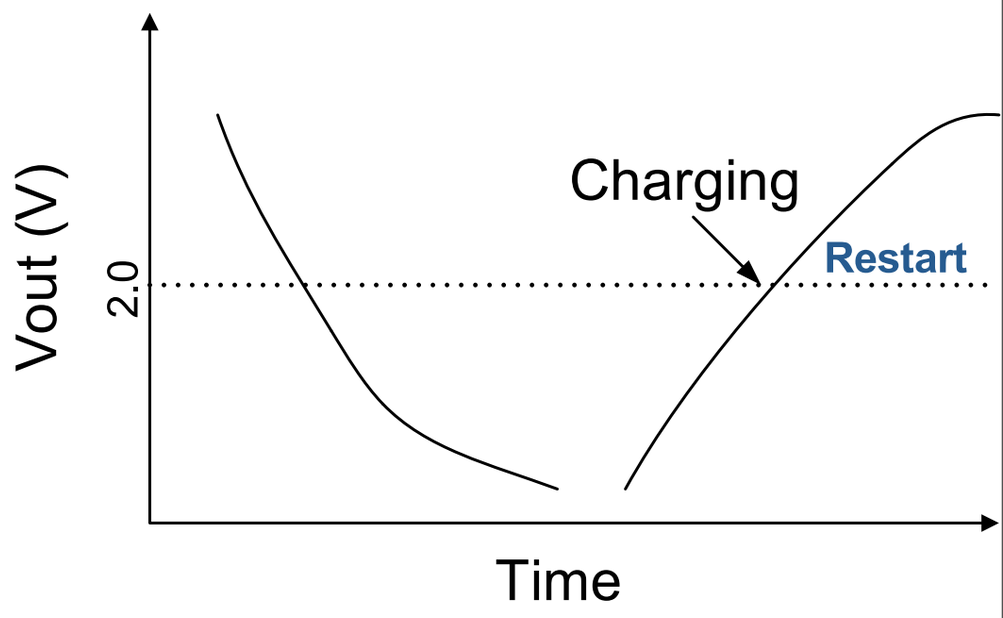
- Voltage Regulator

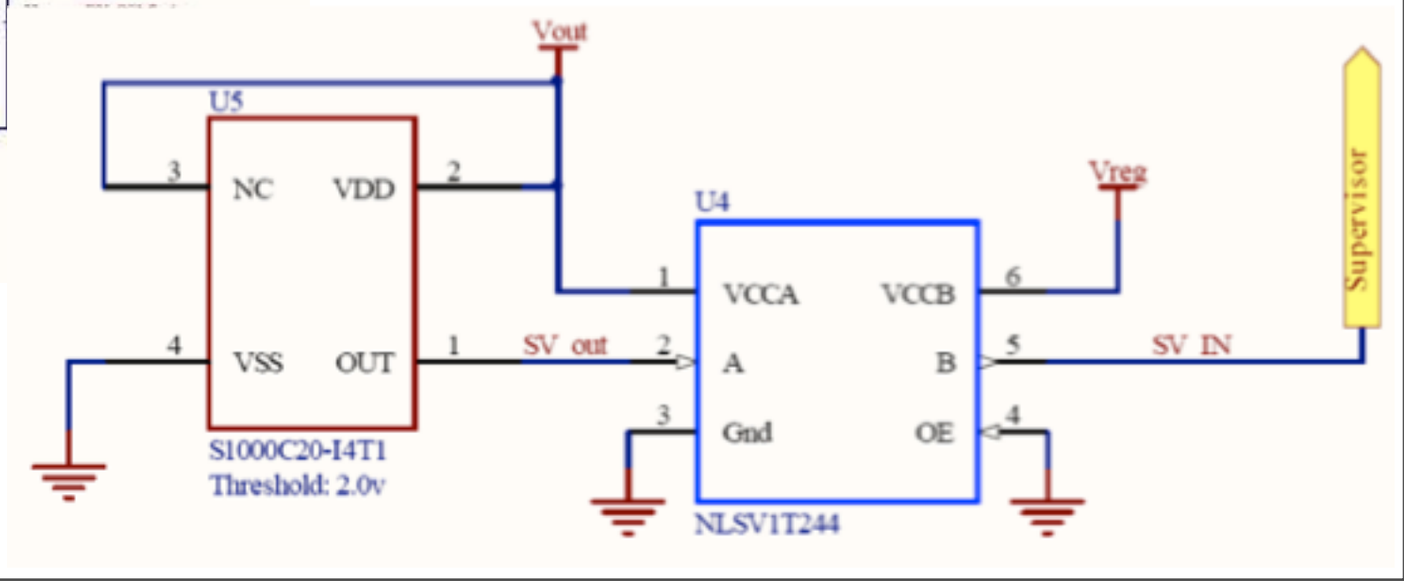


1. How does Moo 1.1 work?

- MSP430 Micro-Controller

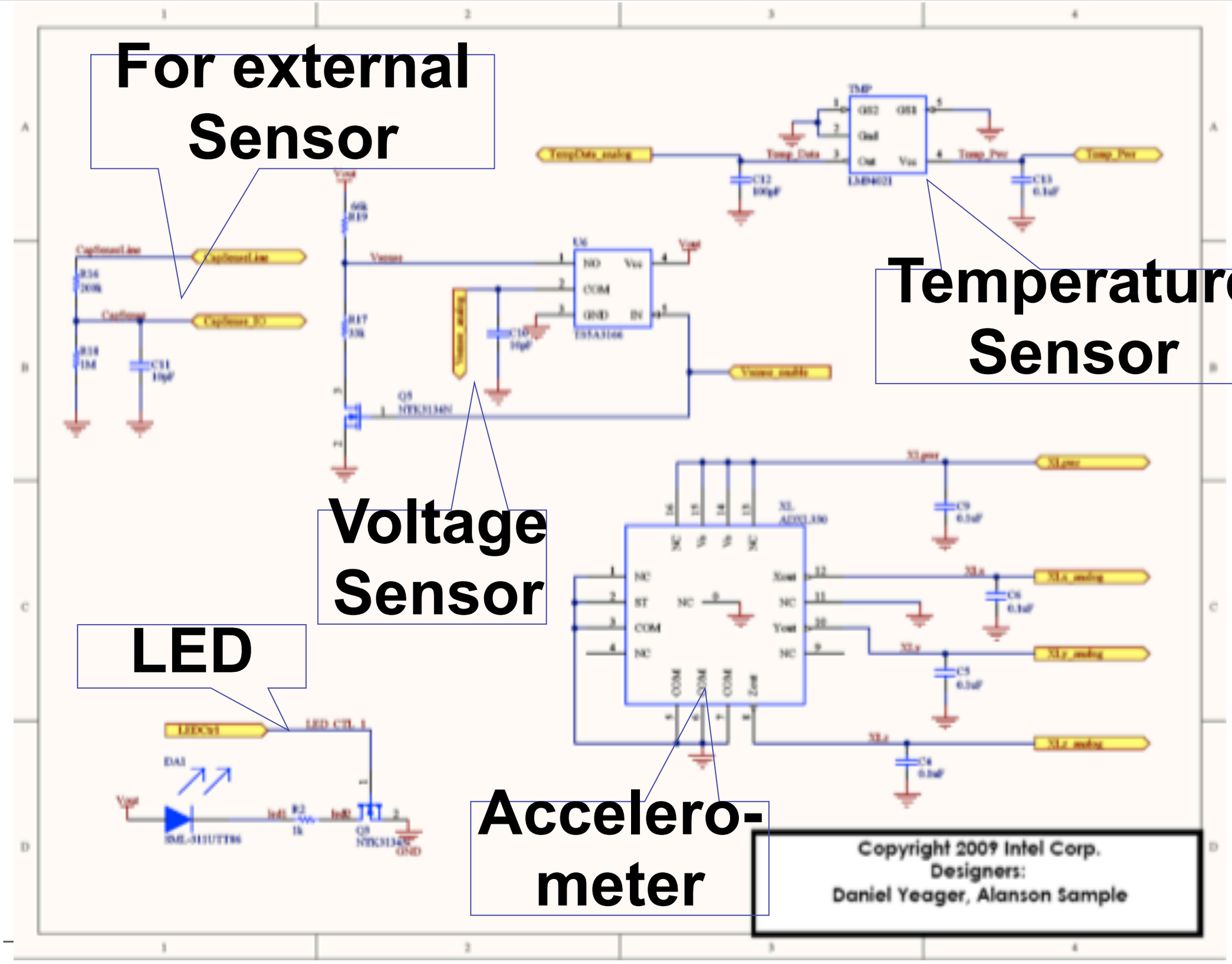






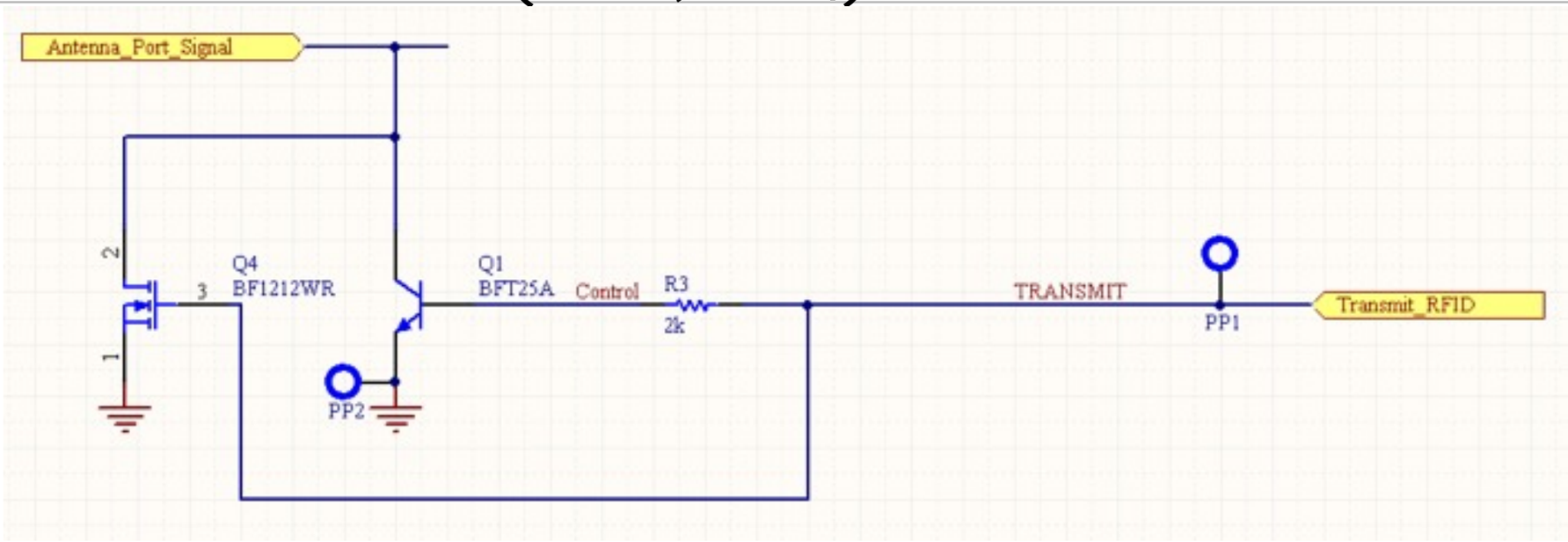
1. How does Moo 1.1 work?

- Sensors



1. How does Moo 1.1 work?

- Modulator (ASK, M=4)



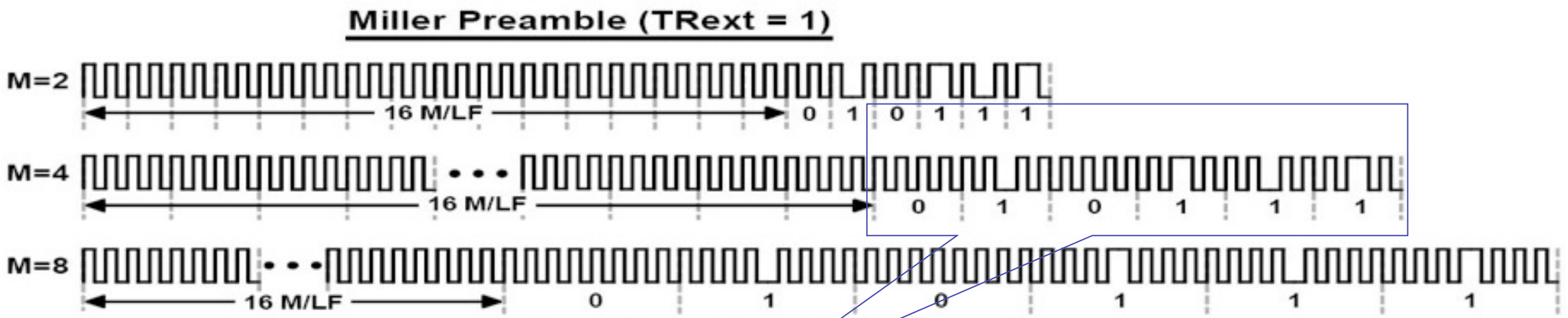
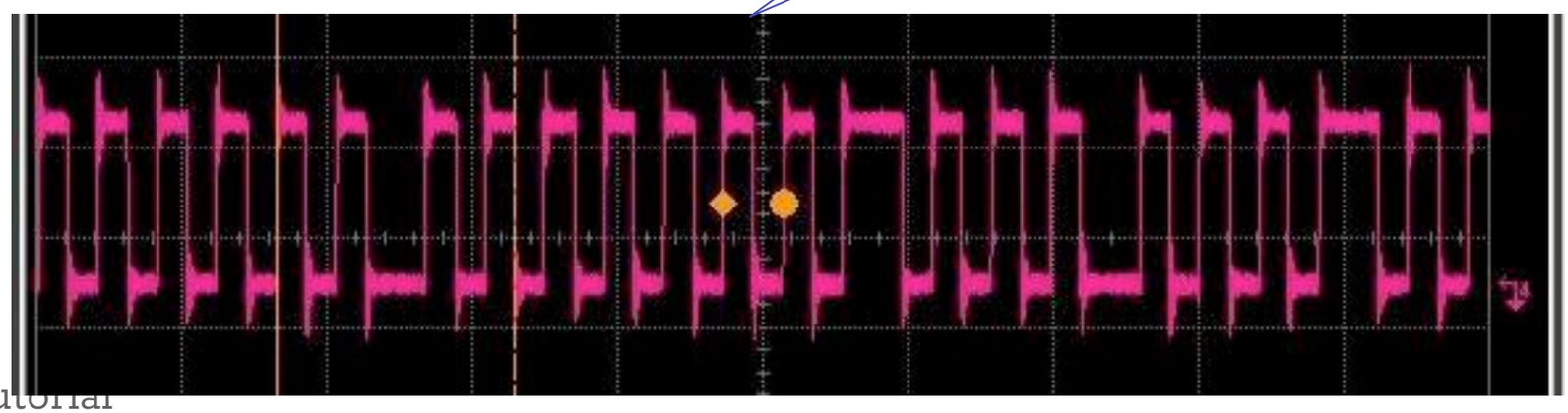


Figure 6.15 – Subcarrier T=>R preamble



2. What are the Moo 1.1 internals?

- MCU: MSP430F2618

MCU		MSP430F2618
Package		64-PIN QFP
Memory Size	Flash	**116KB+256B**
	RAM	**8KB**
Power Consumption	Supply Voltage	1.8V to 3.6V
	Active Mode	365uA@1MHz, 2.2V
	Standby Mode	**0.5uA**
	Off Mode	0.1uA
Architecture		16-Bit RISC Architecture 62.5ns Instruction Cycle Time 32-kHz Crystal 12-bit ADC/DAC
ADC	Supply Voltage	2.2V ~ 3.6V
	Supply Current	0.65mA@2.2V, 0.8mA@3V

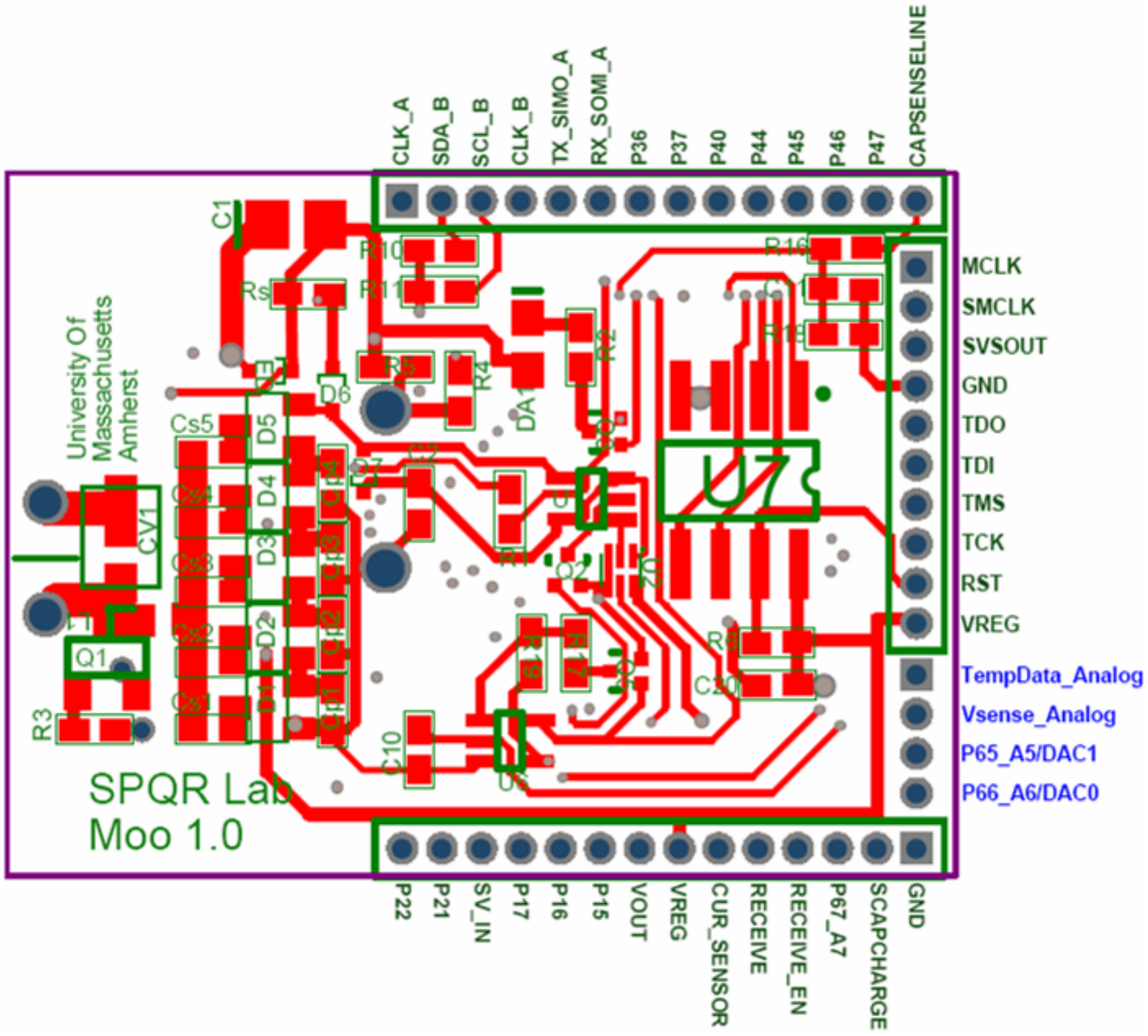
2. What are the Moo 1.1 internals?

- Memory: External Flash

Type #	SST25WF040
Description	On Moo 1.0
Memory Size	4M (512K x 8)
Speed	<= 20MHz
Supply Voltage	1.65v ~ 1.95v
Active Current	2mA @ 20MHz
Standby Current	2uA
Interface	SPI Compatible: Mode 0 and Mode 3
R/W/E time	Byte program (Byte Write): 50us Chip-erase: 125ms Block-erase: 62ms
Package	8-lead SOIC (150 mils)
Size	LxW = 5.80mm x 5.00mm

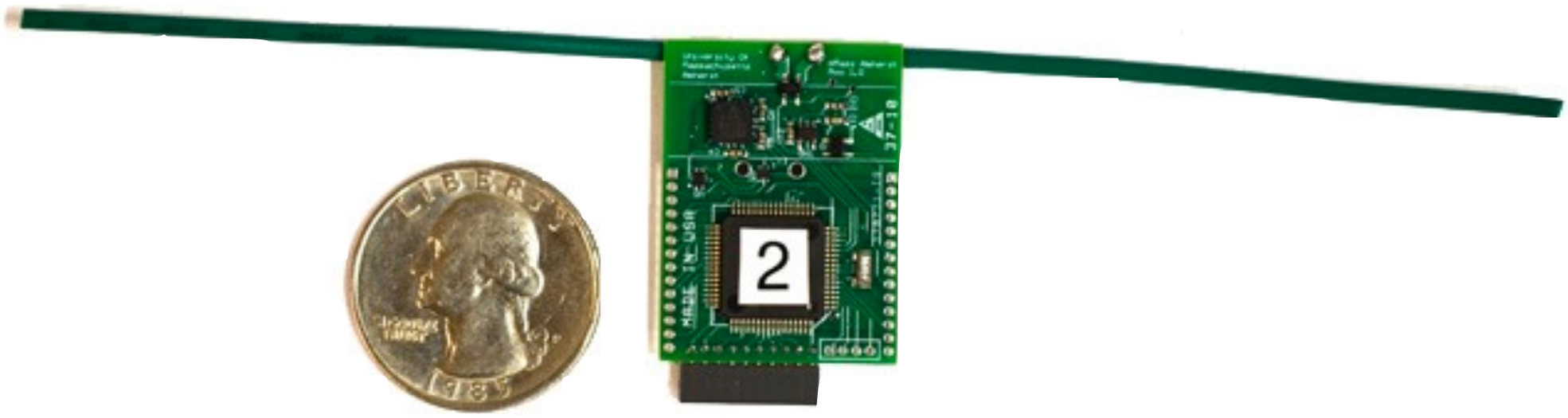
2. What are the Moo 1.1 internals?

- 42 I/O Ports: GPIOs, ADC/DAC, SPI buses



2. What are the Moo 1.1 internals?

- Size: Moo 1.1 vs a quarter dollar coin



2. What are the Moo 1.1 internals?

- Some estimation about power consumptions
  - When Moo 1.0 is about 1.3ft from RFID reader, the power harvester can harvest about (3V)^2/(12.65kOhm) = 0.7mW. The current is about 237uA.
  - When the 10uF capacitor is fully charged, it has a voltage of about 5.4V. Before the voltage of it drops to 3V, it can provide (5.4^2-3^2)/2*10^(-5) = 0.1mJ
  - When Moo 1.0 works actively and ADC is converting, the power consumed is about 3V*(365uA+0.8mA) = 3.5mW
  - With a full charged capacitor and harvesting from RFID reader at 1.3ft above, a rough estimation of continuous work time of Moo 1.0 is: 0.1mJ/(3.5mW-0.7mW)=35.7ms
  - Without harvesting, the work time is: 0.1mJ/3.5mW = 28.6ms

3. What can do in the future?

- Antenna shape
  - Dipolar vs Meander

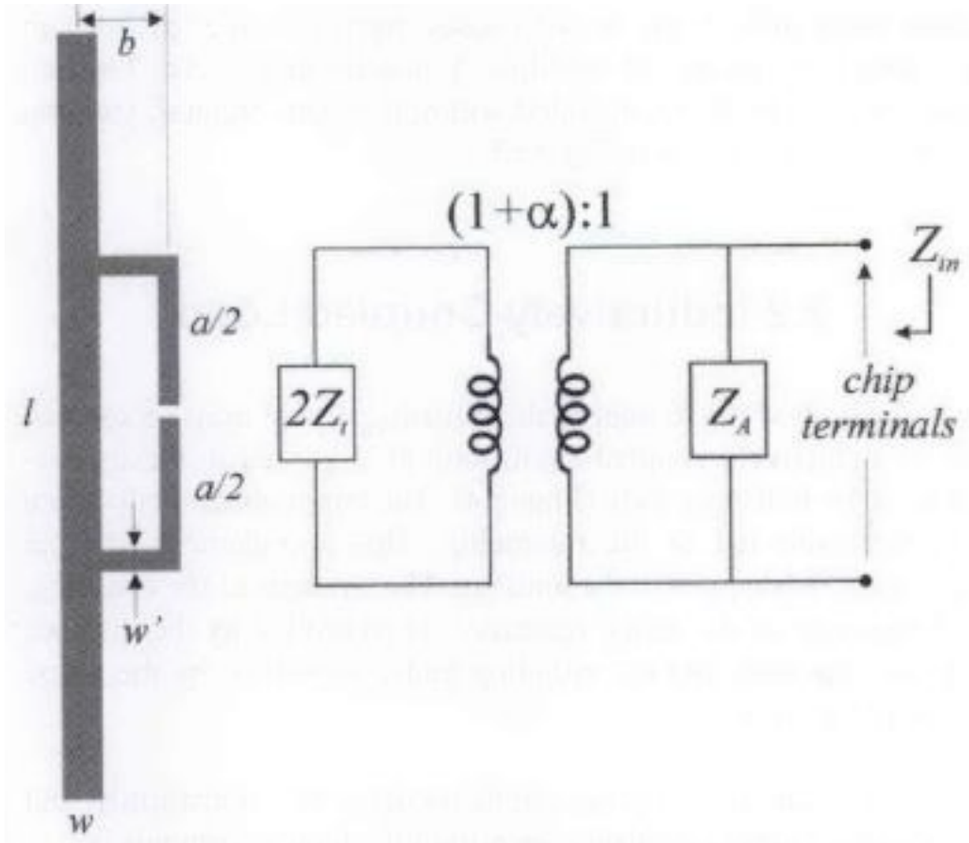


Figure 1. The T-match configuration for planar dipoles and the equivalent circuit, where the impedance step-up ratio $(1+\alpha)$ is related to the conductors' cross sections.

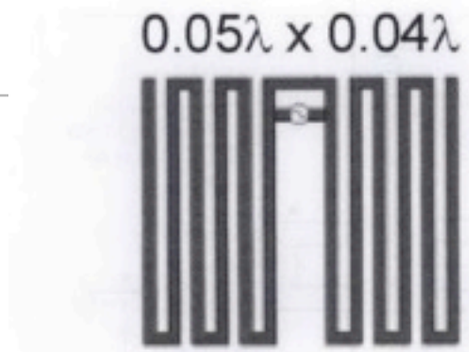


Figure 9a. An equi-spaced meander-line antenna.

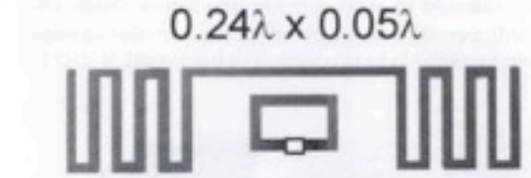


Figure 9b. A meander-line antenna with an inductively coupled loop feed.

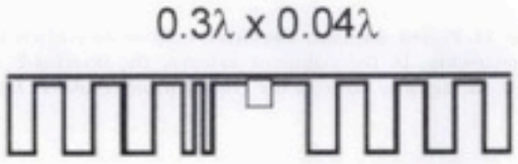


Figure 9c. An equi-spaced meander-line antenna with a loading bar.

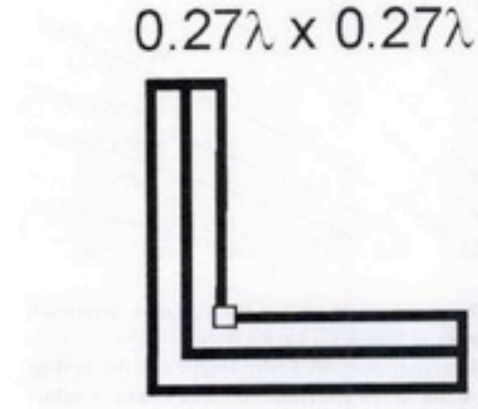


Figure 9d. A doubly-folded L-shaped dipole.

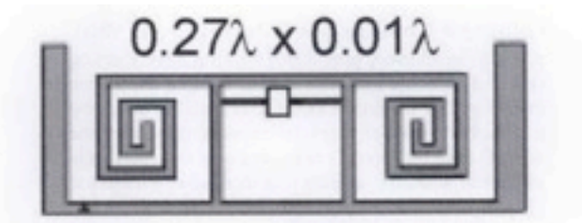


Figure 9e. A multiconductor antenna with a double T-match scheme and spiral folding.

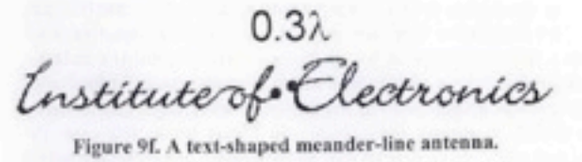


Figure 9f. A text-shaped meander-line antenna.

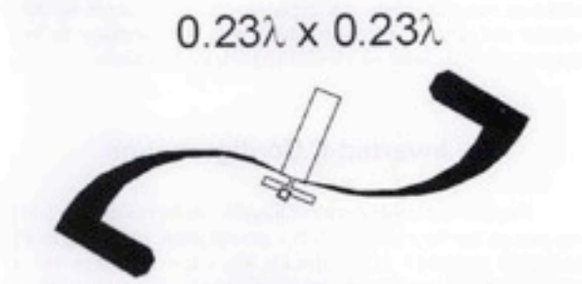


Figure 9g. A resonant tapered dipole that is partially meandered, with a resistive shorting stub and a double inductive stub.

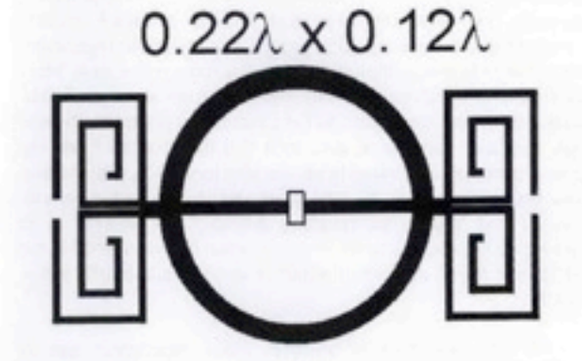
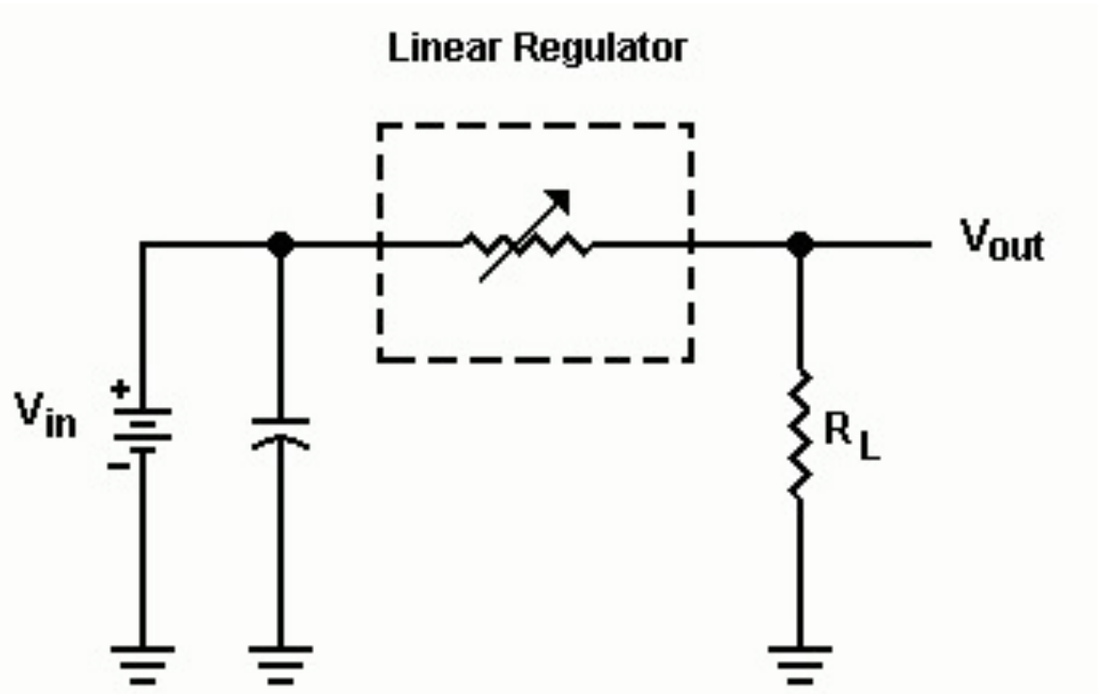
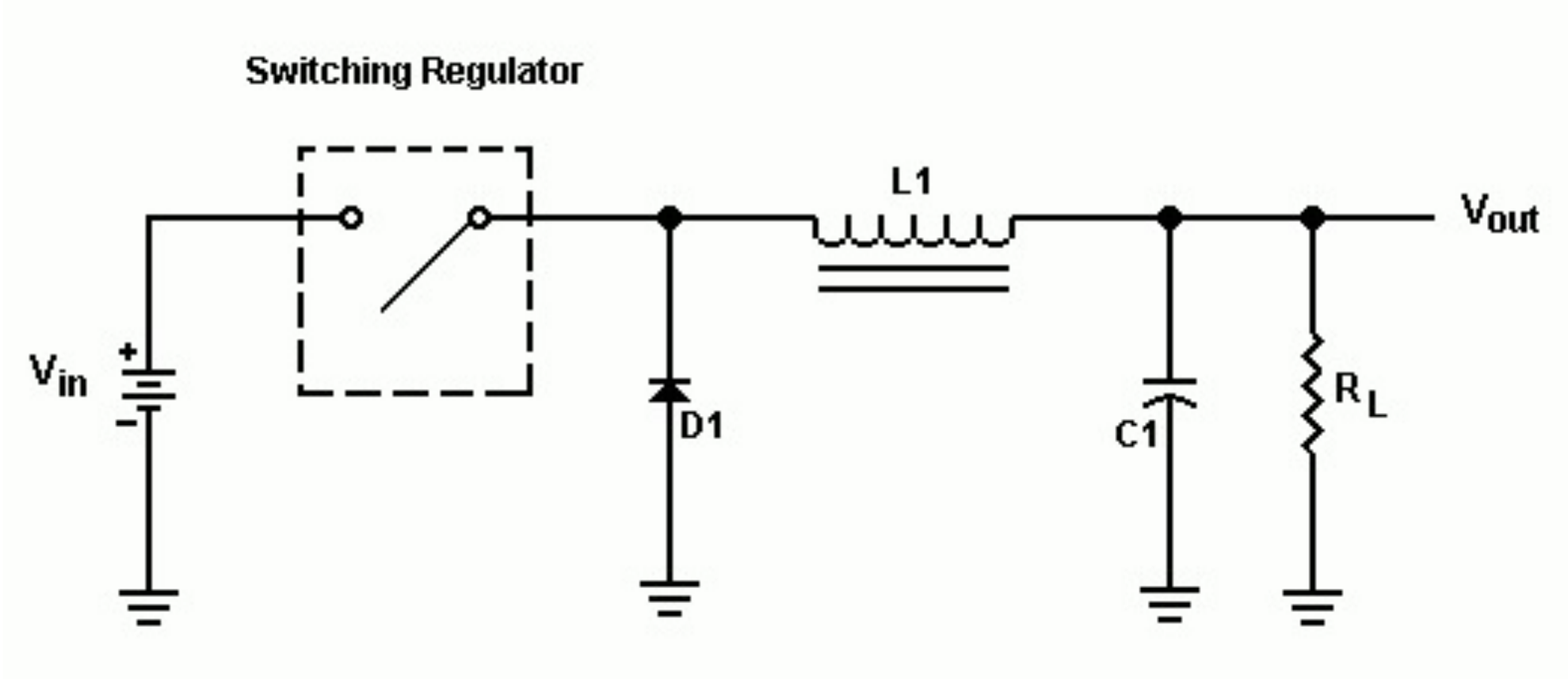


Figure 9h. A multiconductor meander-line tag with a circular-shaped double T-match.

3. What can do in the future?

- Regulator
  - Linear vs Switch





Moo Limitations

- Portions of the C1G2 protocol not implemented
- Strongly constrained by energy availability
  - 0.1mJ/3.5mW = 28.6ms of computation before death

Moo Flexibility

- Options
  - Sensors
  - Harvesters
  - Analog frontend
  - Energy storage (capacitor size, batteries)

“Typical” Moo Programs

- Sensing
- Computation
- Layering protocols on top of C1G2 (will not be covered)

Programming the Moo

- Supported tools
  - Just IAR unfortunately
  - CCR might work with some effort
- Reader programming
  - Impinj and Intel use LLRP (an abomination)
  - ThingMagic uses a C API
  - You can get the code from github
    - https://github.com/spqr

Programming the Moo

- Setting up the development environment
  - VM configuration
  - Getting code from Github
  - Using the reader application
  - Using IAR to setup a project and flash the Moo

A Firmware Tour

- Reader interrupts
  - Comparator and timer
- Timer interrupts
  - For sensing, waiting for ADC

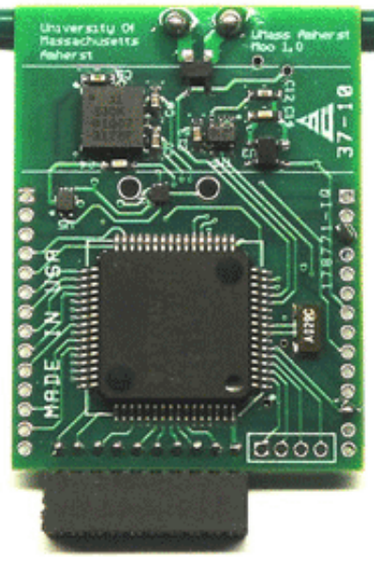
RFIDsec 11

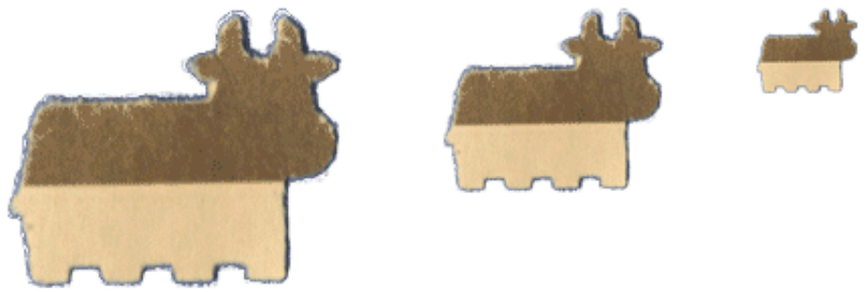
Coffee Break

http://spqr.cs.umass.edu/moo

UMass Moo:

Batteryless
Programmable
RFID-Scale
Sensor Device





Buy a herd from the registration desk.

Photo: www.apartmenttherapy.com