Wireless Communication

with open-source software and hardware

Jared Boone

OSBridge 2012 - June 26, 2012

Topics

Explain the basics of radio communication.

Express how amazing some (all?!) radio technology is.

Demonstrate open-source ways of exploring radio.

~~Consider a few implications of radio everywhere.~~

Do a few live demos if the radio gods cooperate.

Wednesday, June 27, 12

I plan to give you a brief overview of how radios and radio communication works. There's some really cool magic involved in making it all work. And it's getting easier all the time for you to experiment with it on your own.

Topics

...in 45 minutes.

Not at all ambitious!

:-)

To do all of that in 45 minutes means I will leave out so many details, and keep things quite simple. Still, I hope you'll learn some new things and maybe be excited enough to play around with radio a bit yourself.

Who Am I?

Jared Boone, owner of ShareBrained Technology, a (very) small business designing and selling open-source hardware. Presently working on timekeeping, data visualization, audio, and radio projects.

Wednesday, June 27, 12

I own an open-source hardware company. It's just me at this point, designing and selling things I think are interesting -- usually relating to clocks, retro-data display technologies, audio and music synthesis, and, of course radio.

Find the Radios

So where do we find radios these days?

The Obvious

Bluetooth

Wi-Fi

NFC

Flickr: digitpedia

CDMA

GSM

GPS

Wednesday, June 27, 12

Cell phones and laptops, obviously. Cell phones in particular have a ridiculous number of different radio technologies in them. Some of them even have proprietary radios for talking to exercise equipment.

Tire Pressure Monitors

Flickr: jonrawlinson

Tire Pressure Monitoring System

Tire pressure monitoring systems are required on most vehicles manufactured today. I can sit in my house (on a busy street) and see who's got a flat tire.

Restaurant Pagers

I've been handed countless short-distance pagers like this one. What mischief could I make if I knew more about what was inside?

RF Identification (RFID)

Pets, freight, airport baggage, passports, and store merchandise are all being tagged with radio frequency identification tags. I know a guy in my local Dorkbot group who's working on a pet door that opens only for his cat -- using the RFID chip implanted in his pet.

Medical Implants

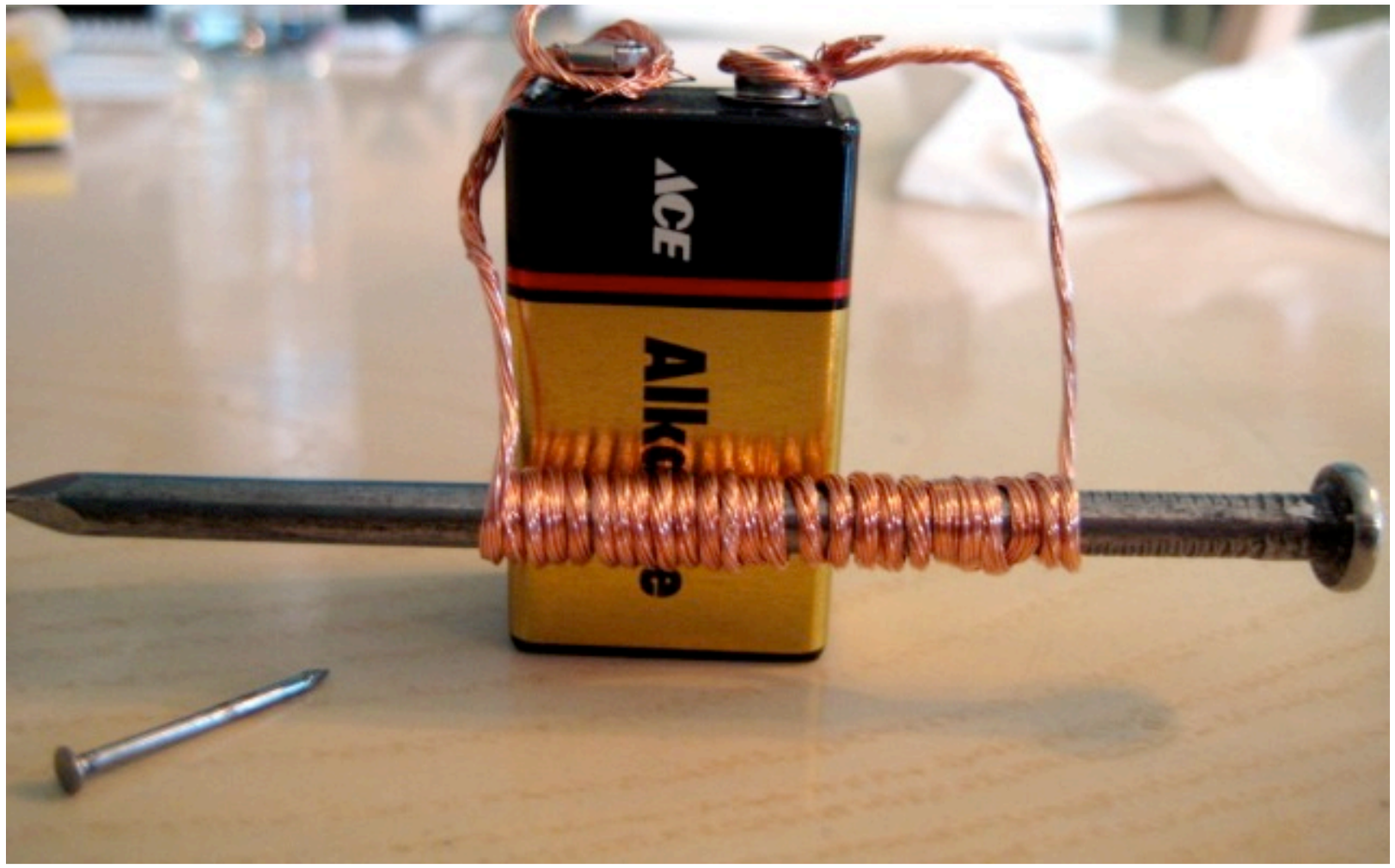
Medical devices implanted inside the body, like cochlear implants and defibrillators, must communicate with the world outside the body in order to function, be programmed, and powered. What are the implications of having a wirelessly controllable device inside your body?

Information Transfer

What is the point of radio? Radio is simply the transfer of information via electromagnetic waves -- "wirelessly".

F***in' Electromagnets

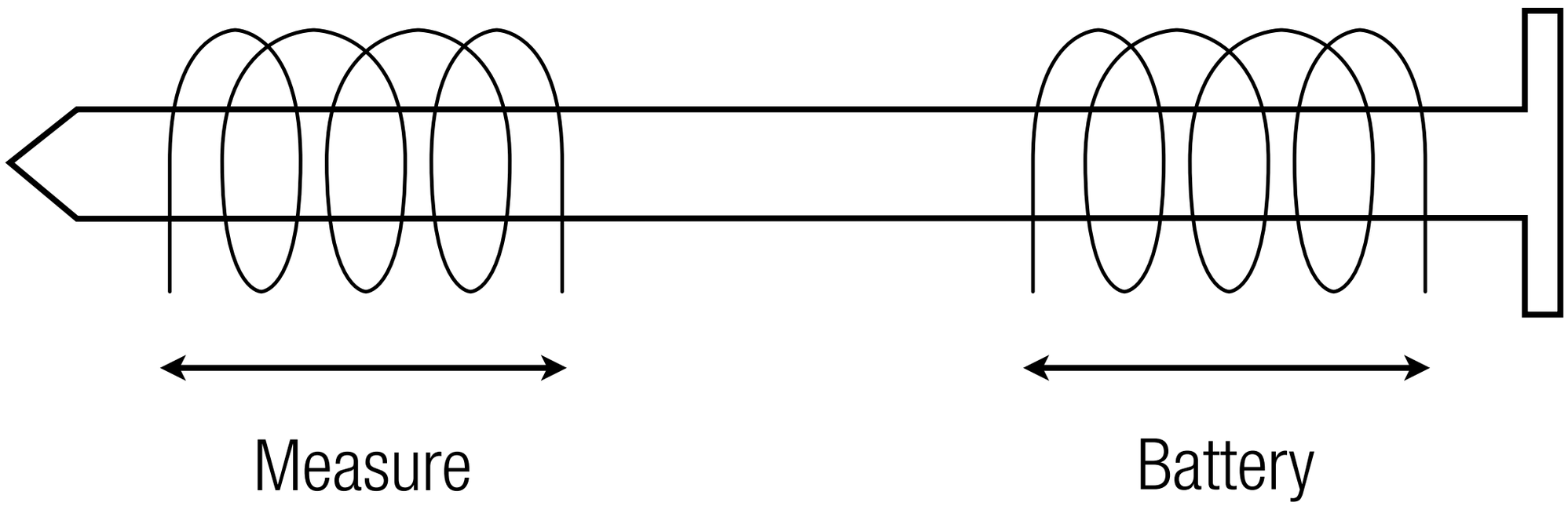
"How do they work?"



Flickr: cobalt_grrl

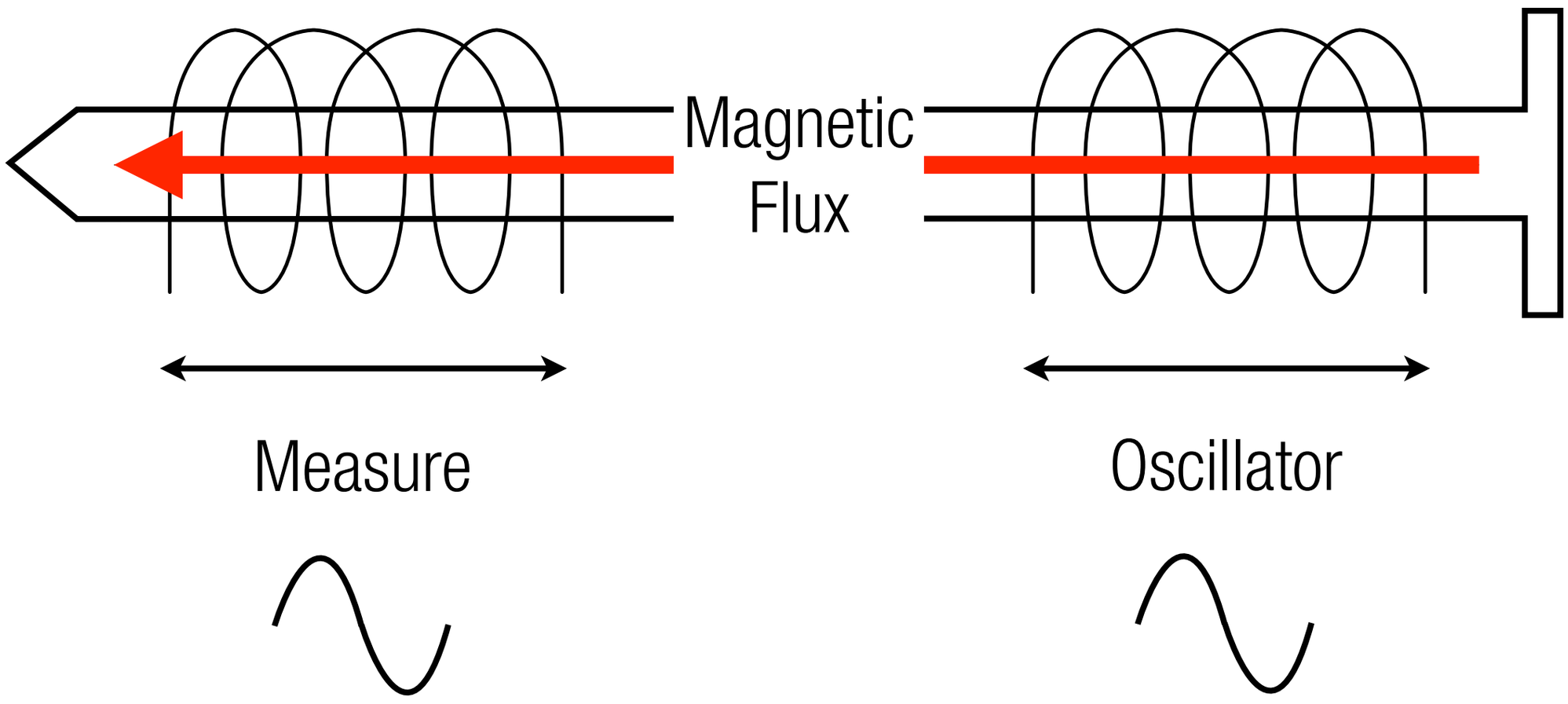
Think back to physics class. You probably made an electromagnet from a nail and a piece of wire. Hook that wire to a battery, and the electrical current flowing through the wire generates magnetic flux through the nail. And the nail becomes magnetic. The more current (the bigger the battery), the stronger the magnetism exhibited by the nail.

Two Coils and a Battery



Now, wrap a second coil of wire around the nail, and measure the voltage across that coil. Hmmm, nothing...

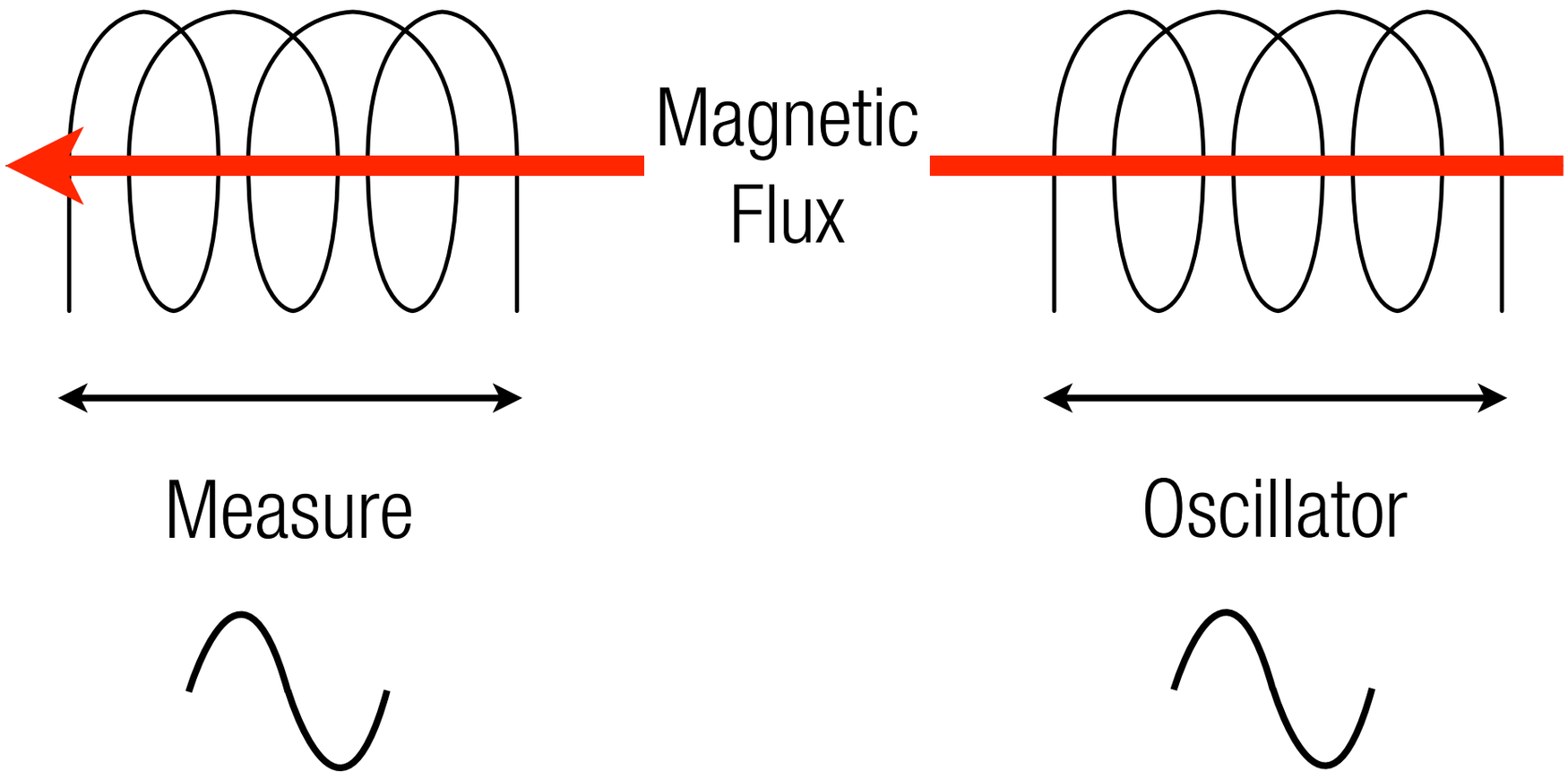
Two Coils and an Oscillator



Wednesday, June 27, 12

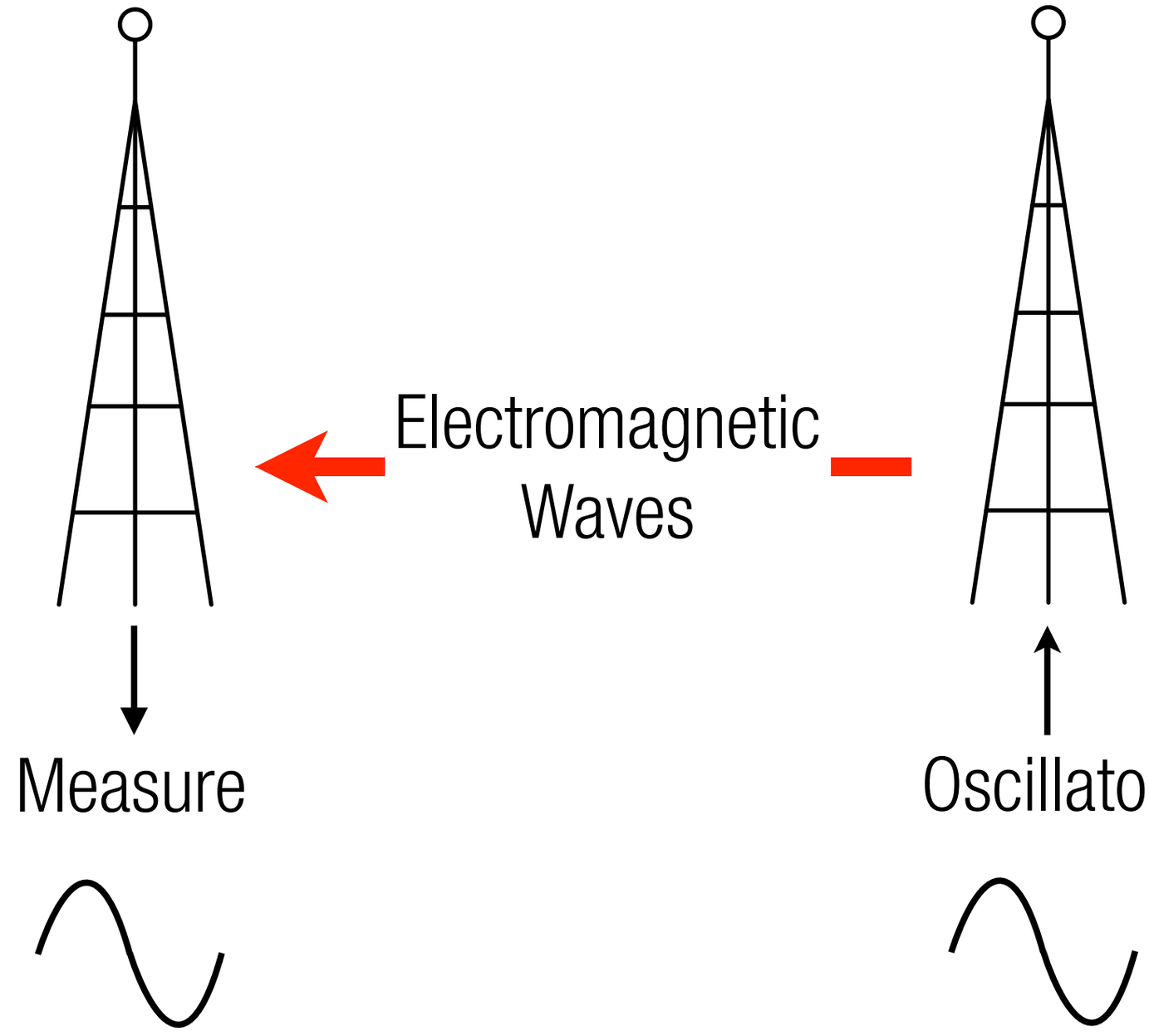
But if we wire an oscillator -- a circuit that generates changing, or “alternating” current at a particular frequency -- we see a similar current flowing through the other coil! We just made a transformer, which is used in just about every piece of equipment that plugs into a wall outlet. Transformers also show up in Ethernet interfaces and audio mixing boards, as a way to separate circuits while still allowing a signal to pass between them. So what if we remove the nail?

No Nail!



Magnetic flux is still generated and still couples between the two coils! Perhaps not as well as when the nail was there, but still, it works.

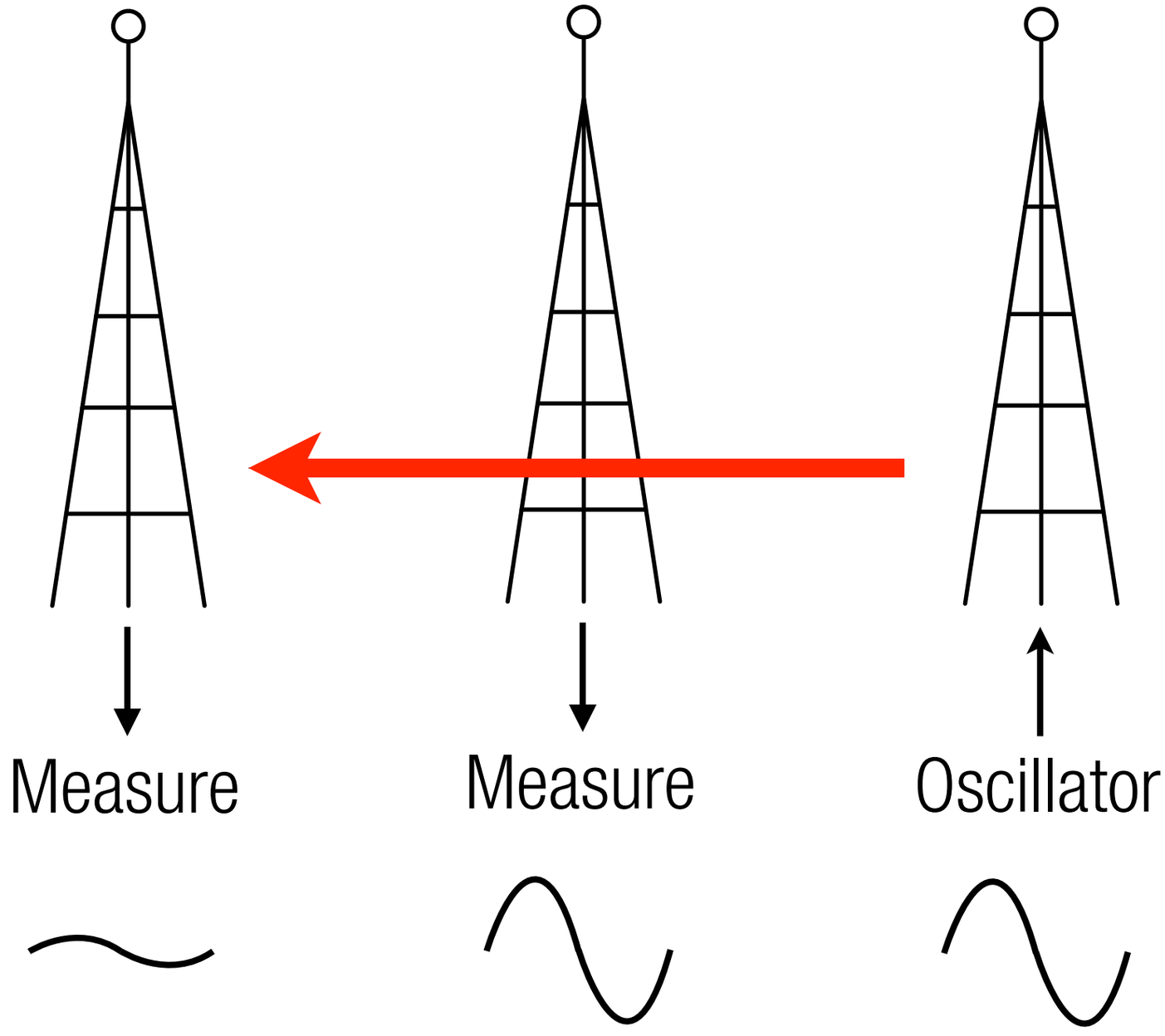
Radio Antennas



Wednesday, June 27, 12

Radio antennas work in a similar way, but at much greater distances.
How far can we separate these antennas? Quite a bit, it turns out.
The power from the source antenna (the transmitter) spreads out in all directions.

Inverse-Square Law



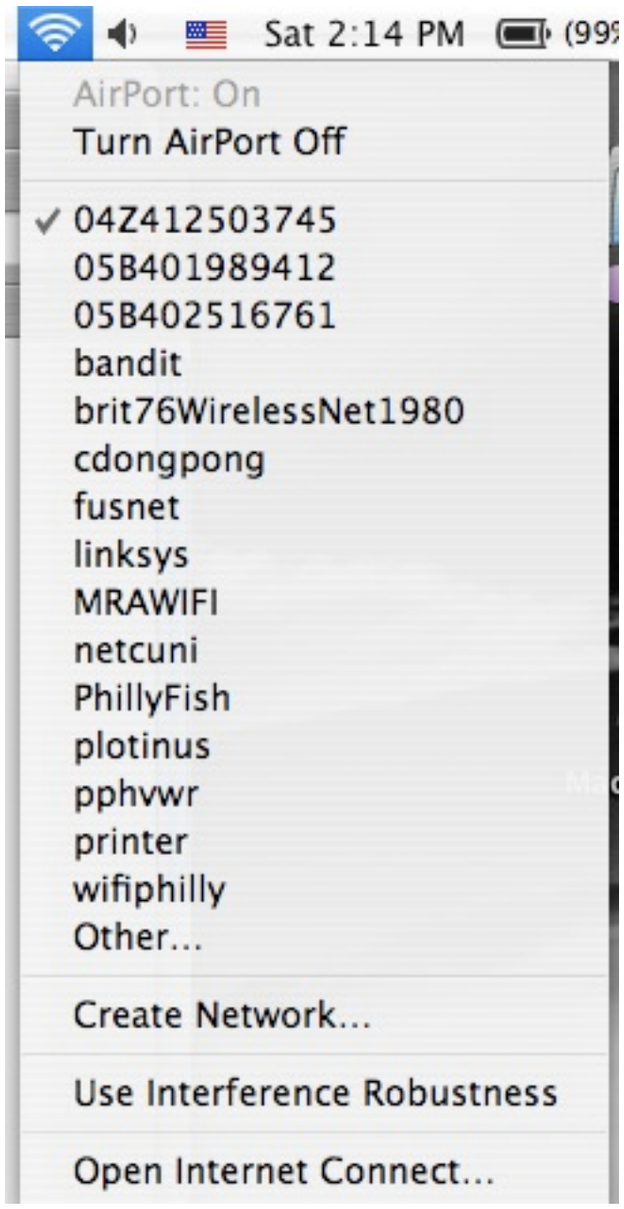
Wednesday, June 27, 12

As the antennas get further apart, the amount of power that reaches the receiving antenna diminishes by the inverse-square law -- an antenna twice as far away will receive one quarter the power. Here's an example. You're 50 kilometers away from a 100,000 Watt FM radio transmitter antenna. The power at the antenna is 100,000 Watts. (A LOT of power!) That 100,000 Watts spreads out in all directions. When that power gets to the receiver, it's much weaker -- only 1 milliWatt -- not a lot of power. That's not even enough power to light up a small LED. Because of this, radio receivers need to be very "sensitive".

Noise

As our antennas get farther apart, and the signals we want to receive get weaker, noise becomes more of a problem. What sources of noise does a radio have to contend with?

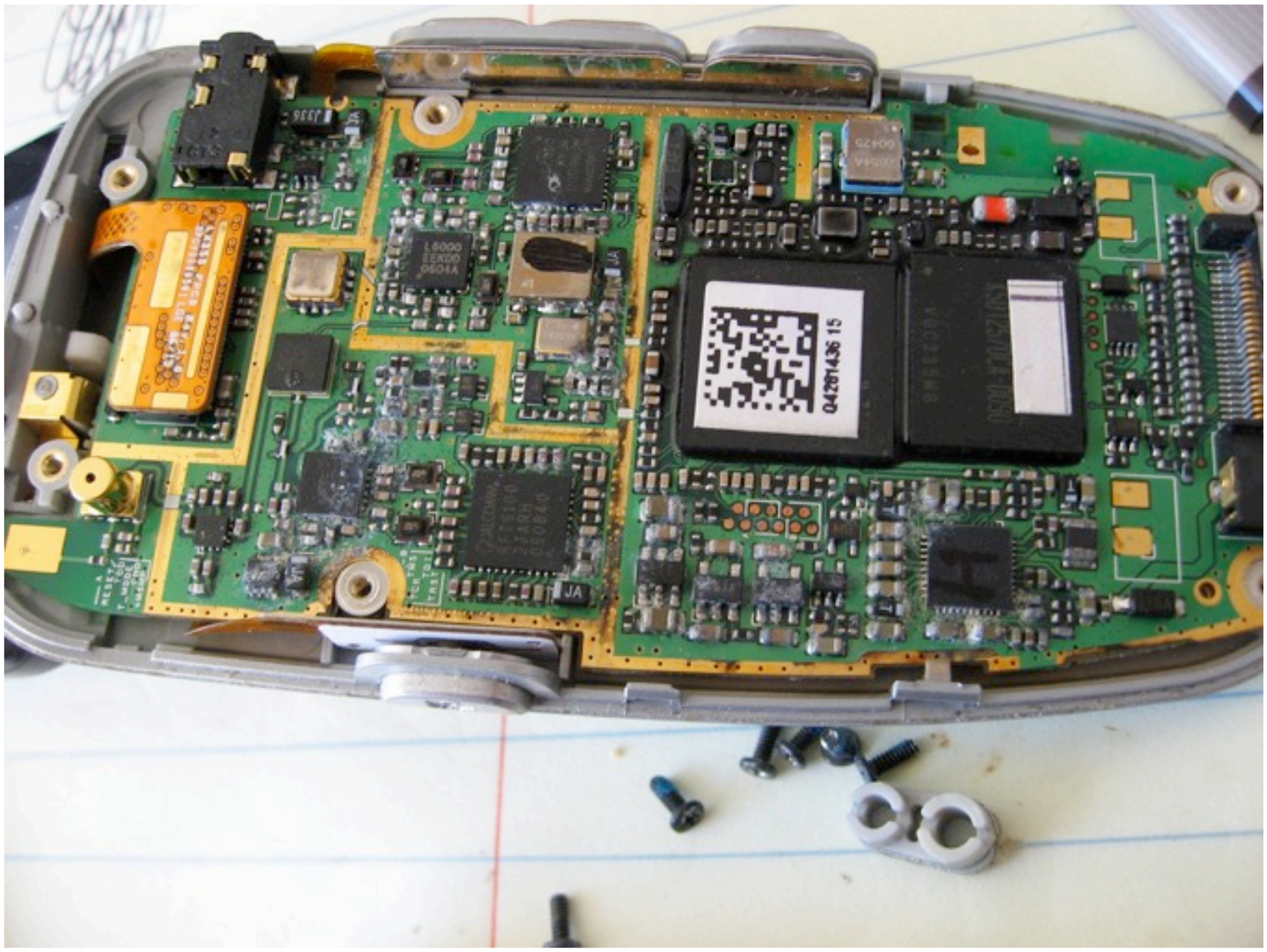
From Other Radios



Flickr: oso

Your neighbor's radios can interfere with yours. We all know how jammed the Wi-Fi band can be... There are a number of clever techniques that can help radios cope with interference from nearby radios on the same frequencies.

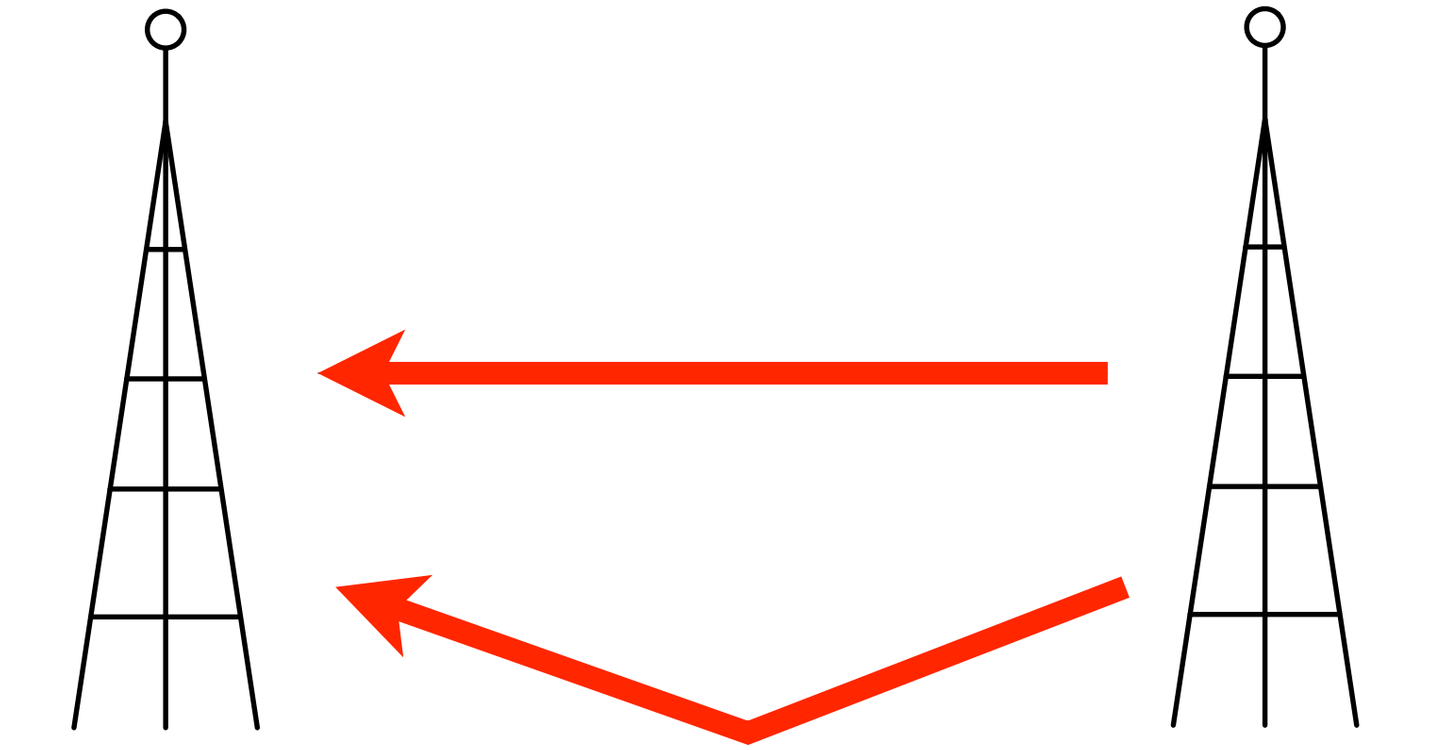
From Your Radios



Flickr: gemstone

Phones and laptops have lots of *different* radios inside -- Wi-Fi, Bluetooth, GPS, cellular all in a single phone. Some of those radios may operate at the same time -- like GPS and Wi-Fi or cellular. Even though they work on different frequencies, they may still interfere with each other if the radios are not designed carefully. Proper frequency filtering inside the radios is the primary way to solve this problem.

Multi-Path Interference



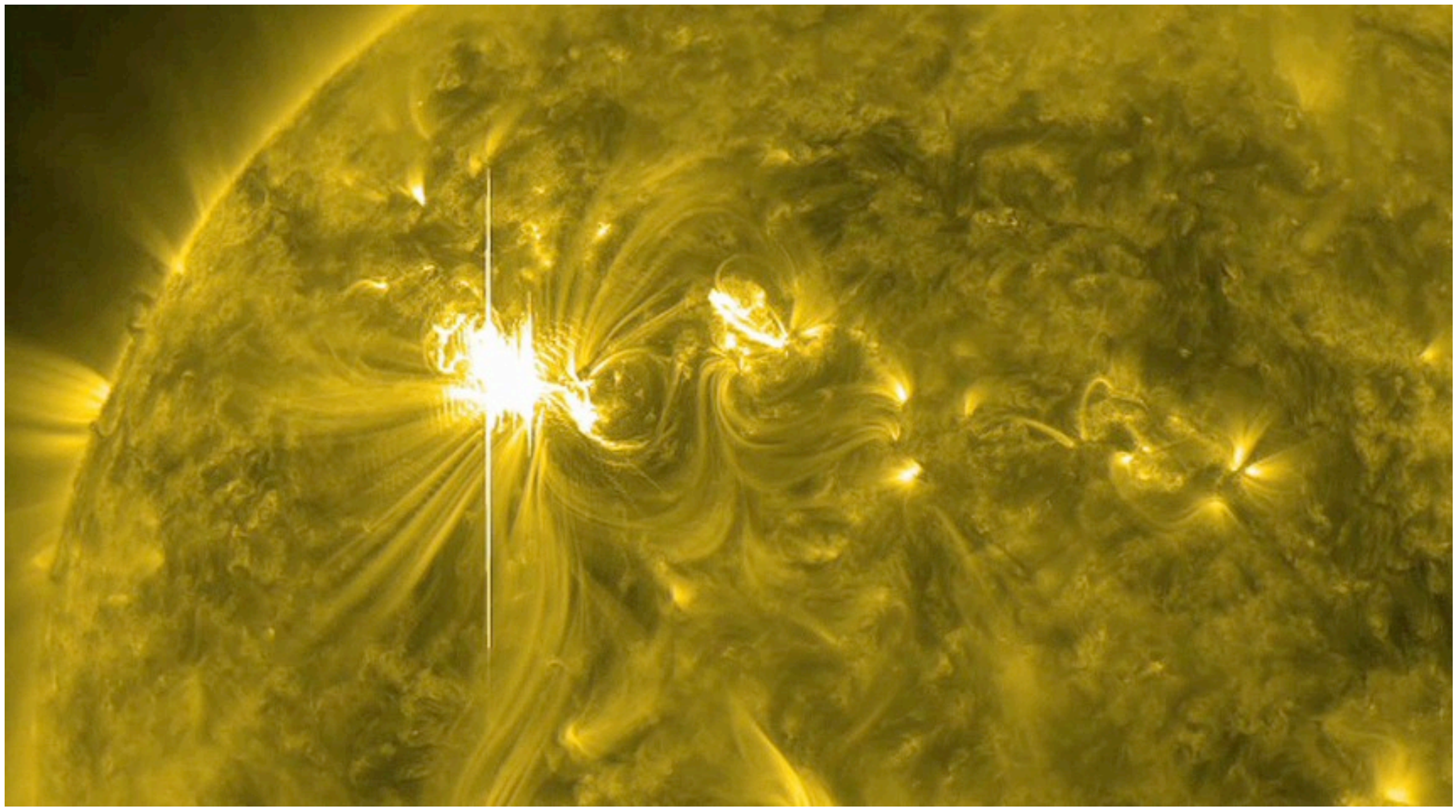
Multi-path interference is caused by radio signals bouncing off of objects -- the ground, hills and mountains, buildings, even passing airplanes! The bouncing signals arrive at the receiver microseconds later than the direct signal. The direct and bouncing signals combine and weaken or clutter up the signal the receiver gets.

Multi-Path Interference

Wikipedia: GraYoshi2x

Back in the analog TV days, multi-path interference caused “ghosting” of the picture.

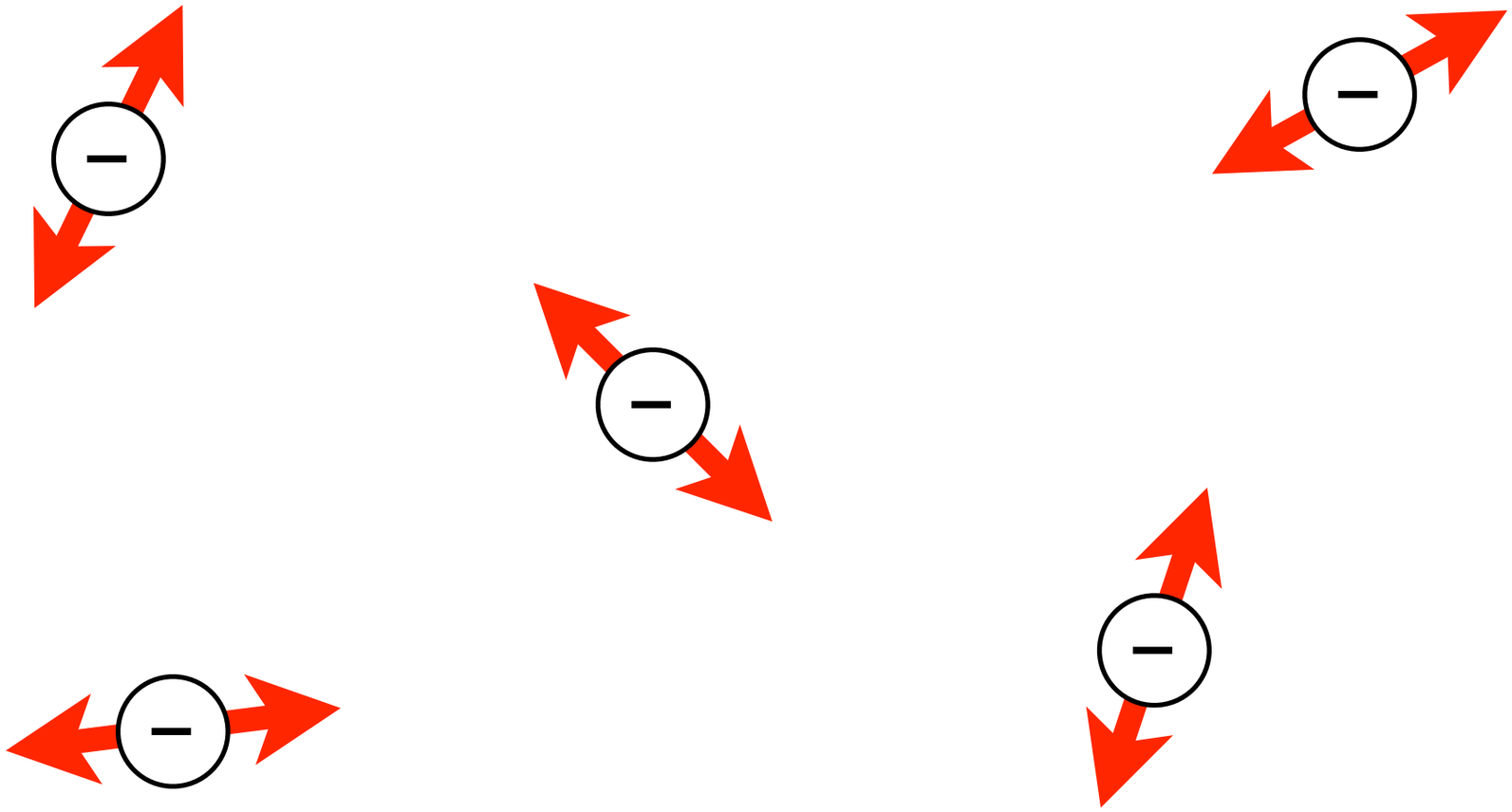
The Sun



NASA/SDO/AIA

The Sun also makes noise, affecting satellites, aircraft navigation, and high-frequency communications. Coronal mass ejections send intense waves of solar particles and magnetic fields that distort the Earth's own magnetic fields. Particularly strong fields cause temporary disruptions in communications.

Wiggly Electrons

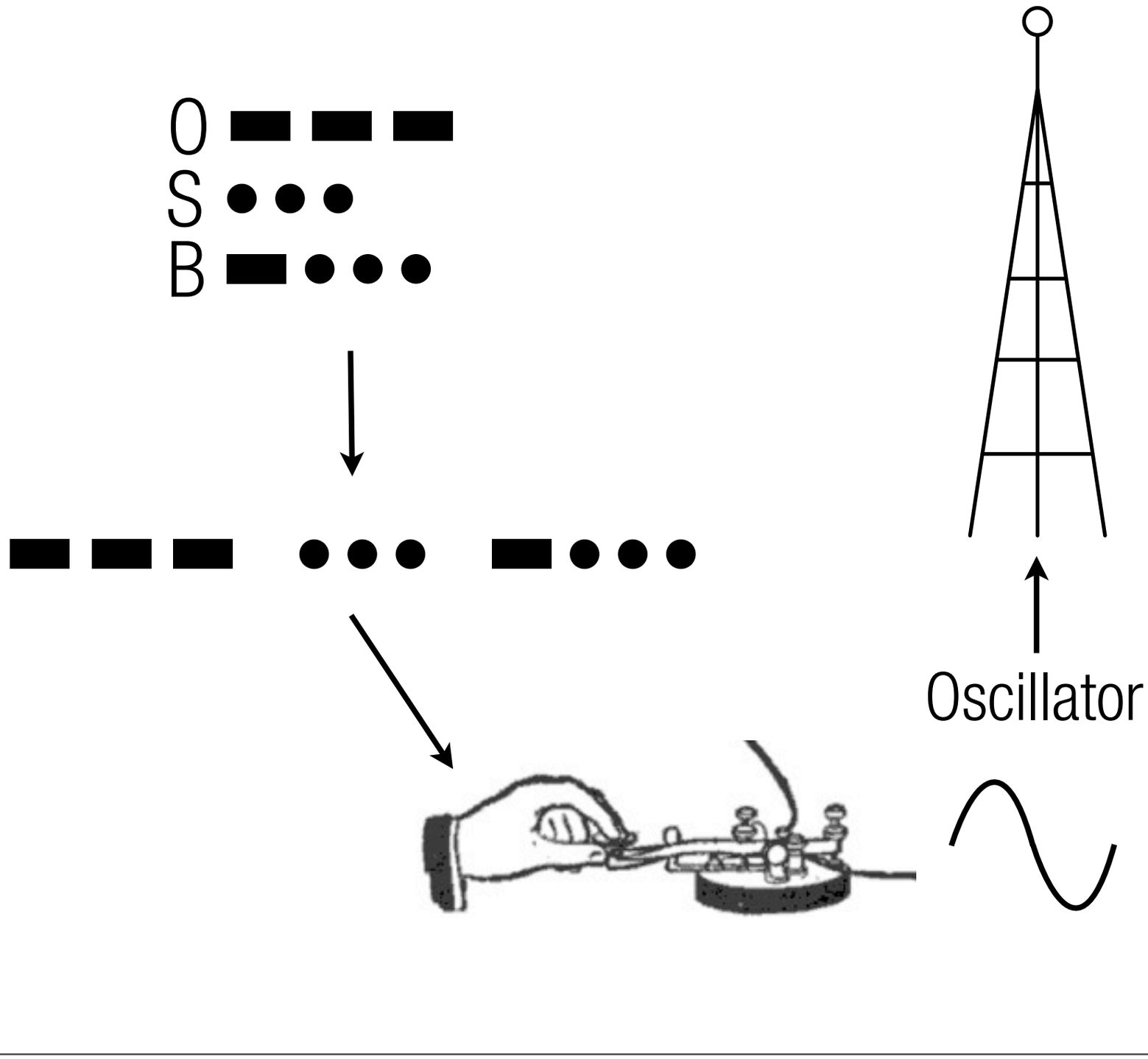


Even the electrons inside a radio are conspiring against receiving a clear, noise-free signal. The electrons inside all circuits bounce around a bit due to thermal energy. This bouncing around produces noise in every circuit. If you cool a radio receiver to very low temperatures, the thermal noise in the circuit is much reduced. Some deep-space radio telescopes do this, because they're trying to receive vanishingly small signals over *literally* astronomical distances.

Modulation

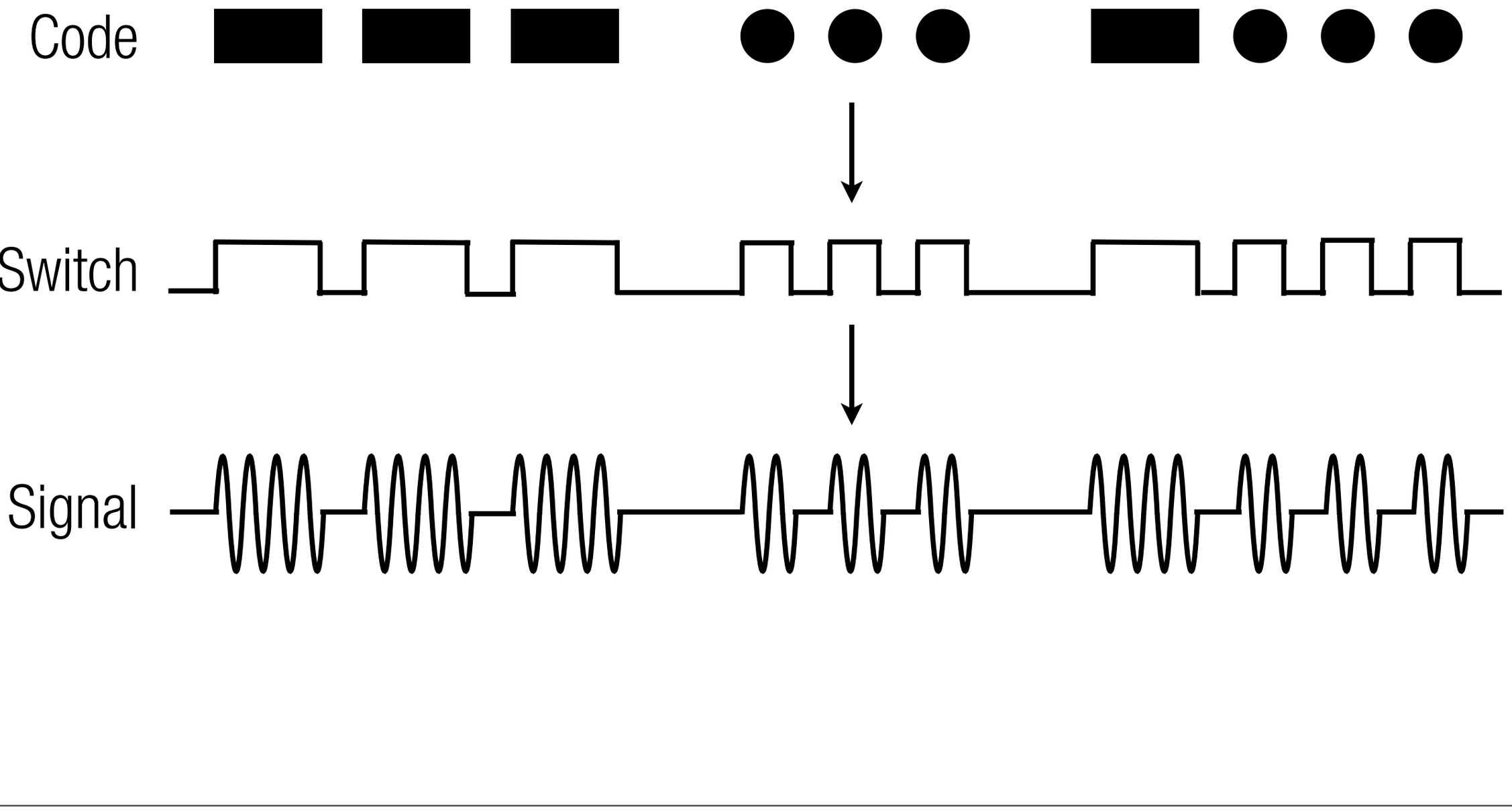
How do we transform data into radio signals that work efficiently and reliably? We chose a modulation scheme that's appropriate for the circumstances -- the kind of data we want to send, how far we need to send the data, how reliable the communication needs to be, and the amount of power we have available to send it.

Morse Code



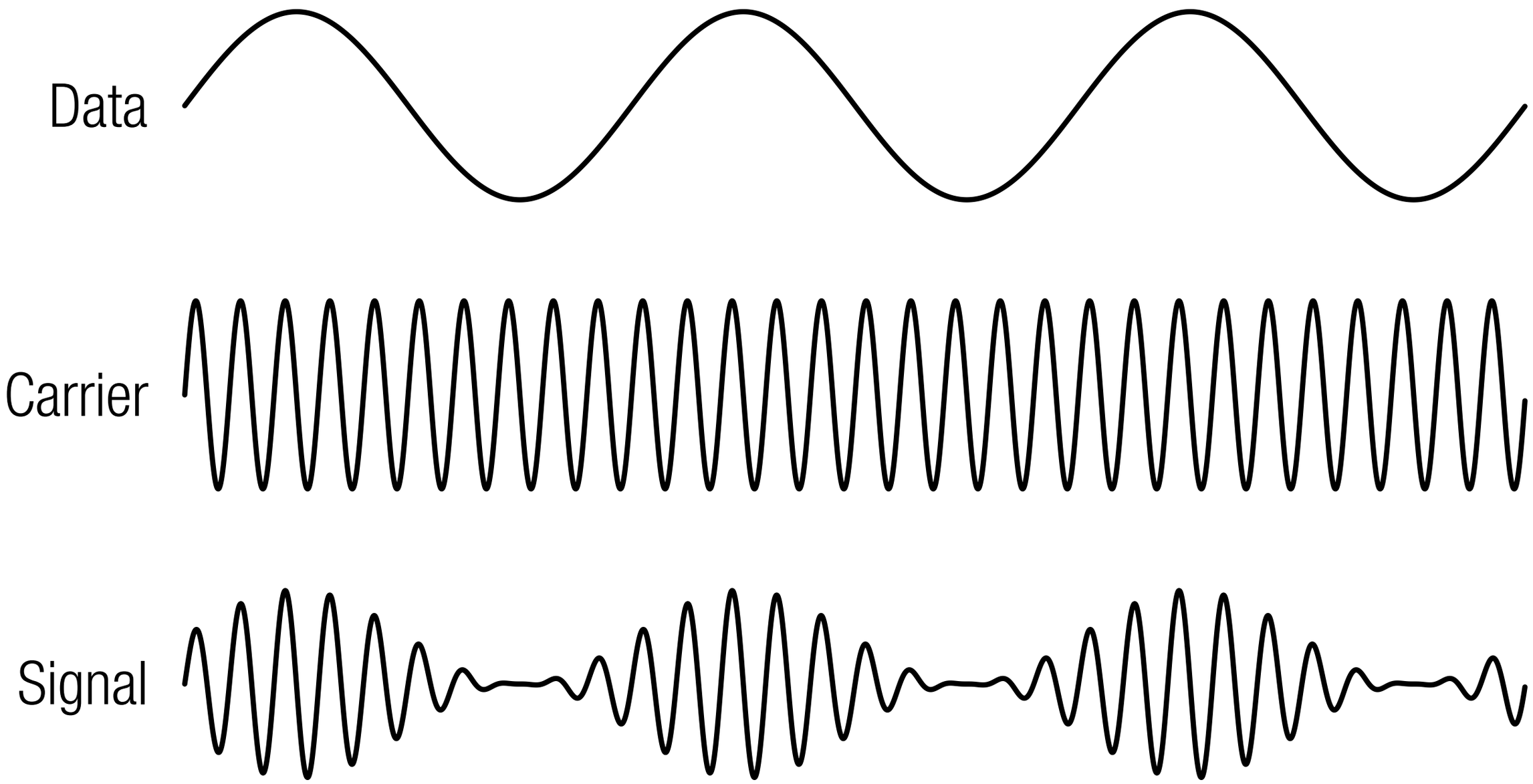
Morse code is perhaps the simplest modulation scheme there is. Take an oscillator, tuned to the frequency you want to transmit on, and turn it on or off according to patterns corresponding to different letters of the alphabet.

Amplitude Modulation



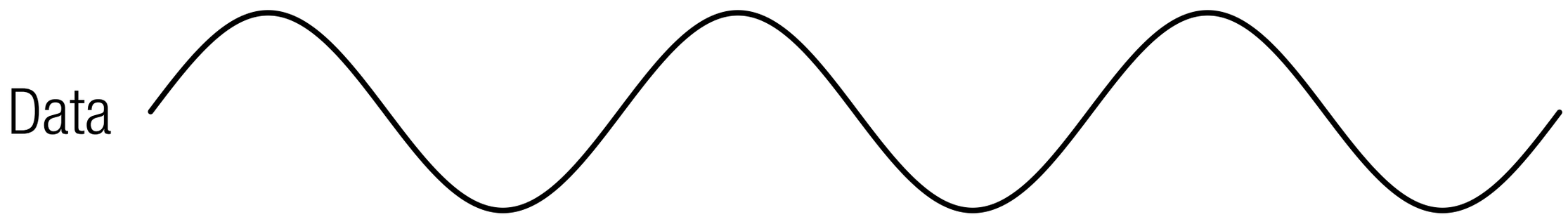
Morse Code is an extreme example of amplitude modulation. When the switch is closed, the oscillator is connected to the antenna -- the amplitude of the transmitted signal is 100% -- full-on. When the switch is open, the oscillator is disconnected from the antenna, and the amplitude of the transmitted signal is 0 -- no signal at all, completely off.

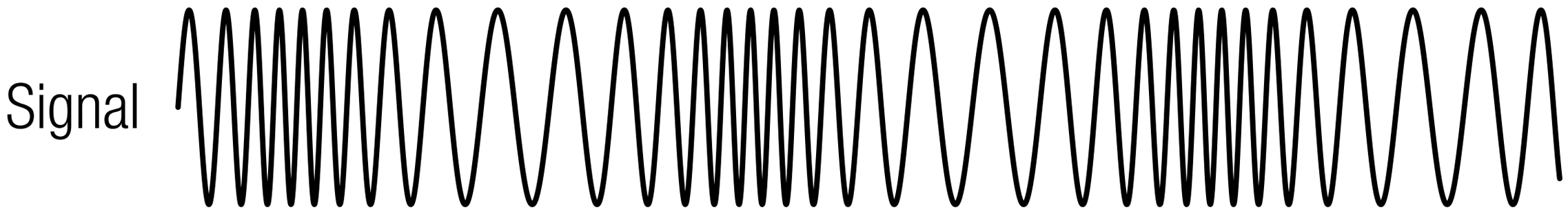
Amplitude Modulation



When the data to be transmitted is not a simple on/off (binary) message, but an analog message (like audio for AM radio), an amplitude-modulated signal looks like this. The amplitude of the carrier is controlled by the data.

Frequency Modulation

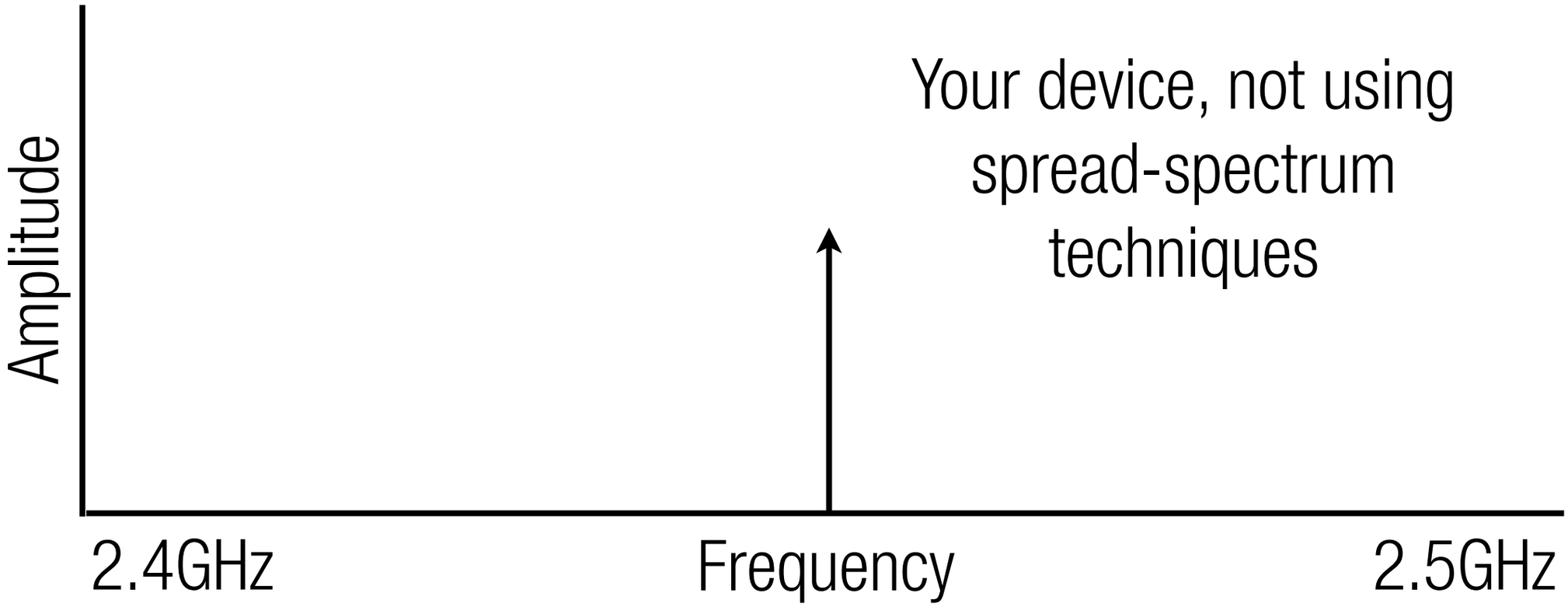




Wednesday, June 27, 12

Frequency modulation uses the data to directly alter the frequency of the carrier. This is where the name “FM” comes from for FM broadcast stations. But FM is used for a lot of other communications -- from cabbie radios to weather satellites.

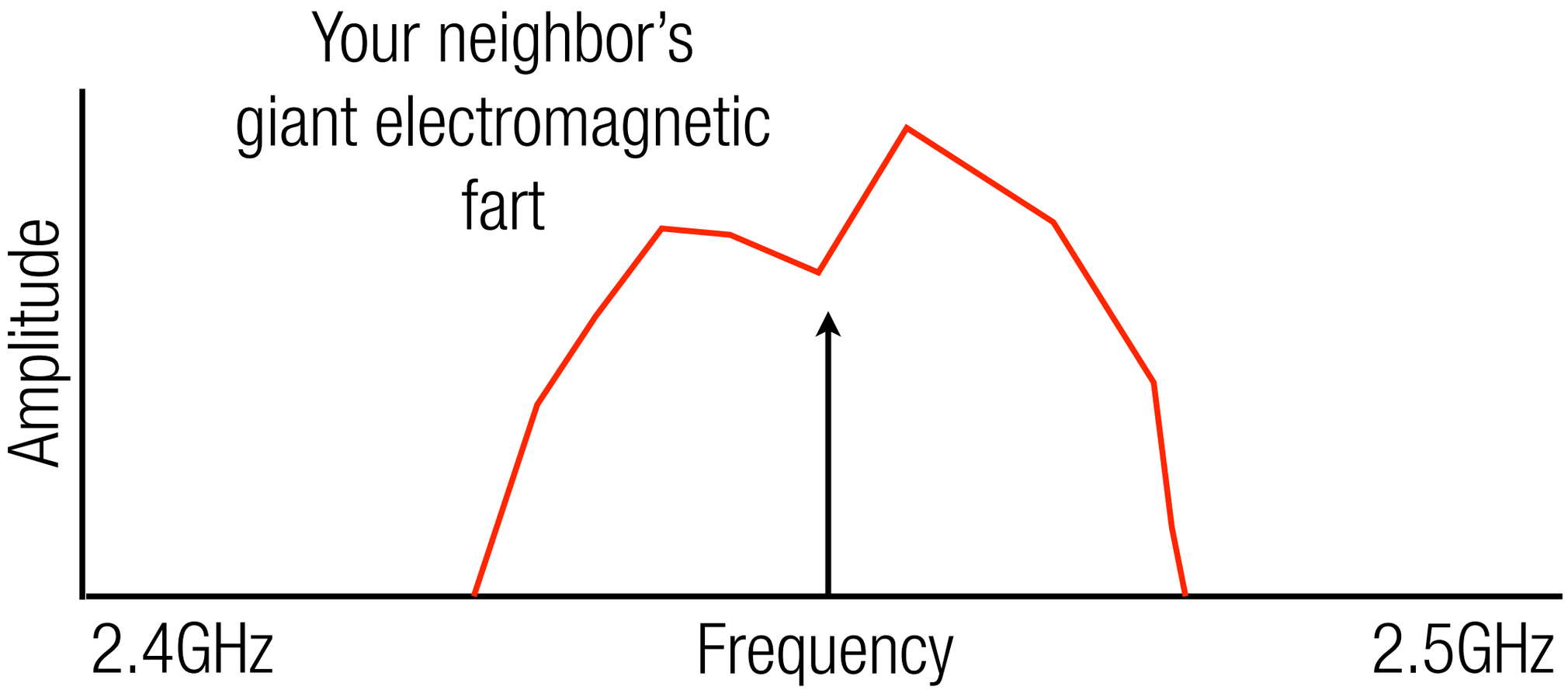
Spread Spectrum



Wednesday, June 27, 12

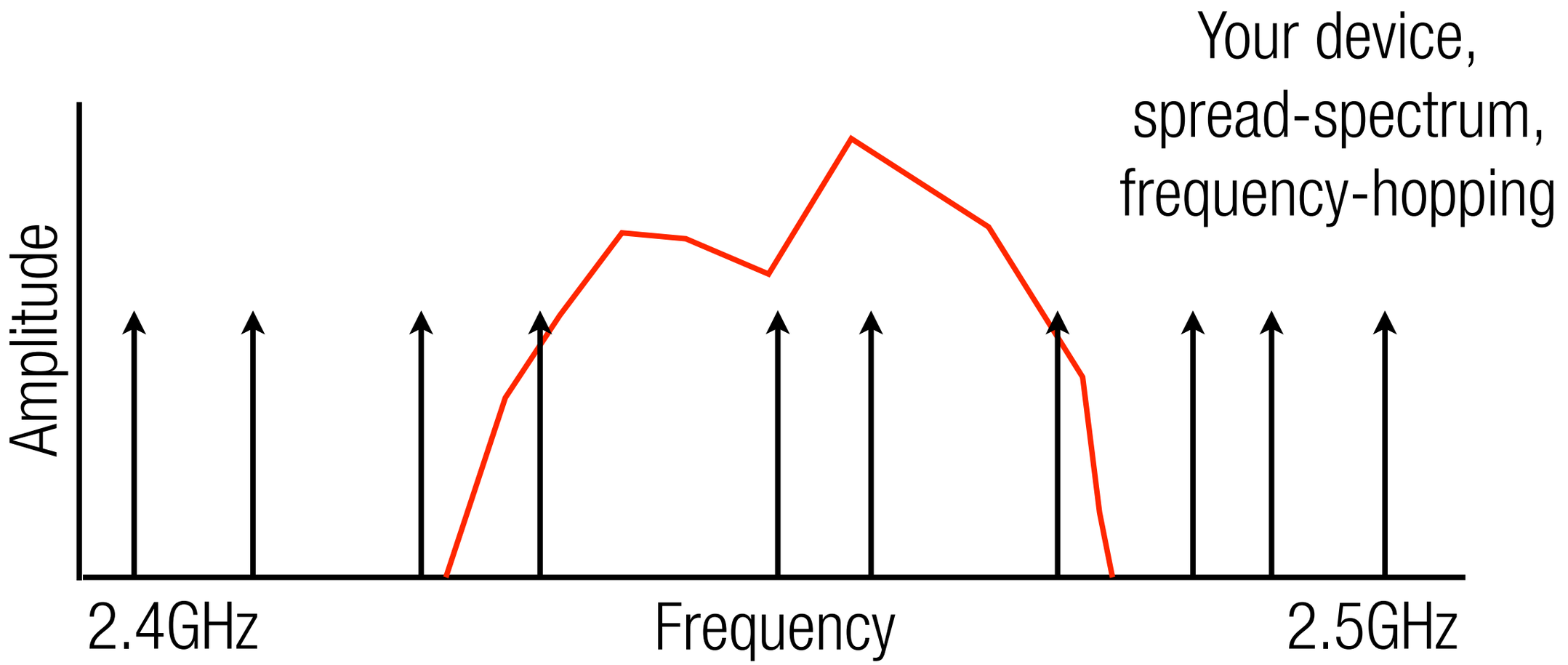
“Spread spectrum” is a technique that deals well with noise from other radios, which is why it’s used so much in the 2.4GHz band, where Wi-Fi, Zigbee, Bluetooth, and even microwaves compete to do their business. Imagine you’re using a radio (maybe an exercise wristwatch) that’s not spread spectrum. Here it is, transmitting in the middle of the 2.4GHz band -- a narrow-bandwidth signal.

Spread Spectrum



Your neighbor turns on their microwave, or maybe they start watching a movie on Netflix over their wireless access point. Now, your computer can't communicate with your exercise watch because it can't hear over your neighbor's noise.

Spread Spectrum



Wednesday, June 27, 12

So we go all Mohammed Ali or Agent Smith on the problem. If we move fast enough, we're harder to hit. We transmit small portions of the data we want to send on different frequencies, in rapid succession. Along with the data, we transmit some redundant information useful for detecting and correcting errors. Some of the transmissions will collide with the neighbor's signal, but many of them will not. Then, we use the extra transmitted data to detect which data is damaged by the noise and repair it.

Thank You Hedy!

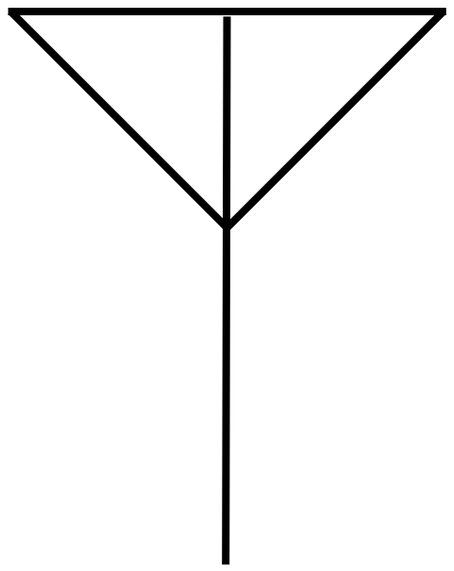
Wikipedia: public domain

And the most interesting thing about spread spectrum? Actress Hedy Lamarr and her composer friend George Antheil invented spread spectrum in the 1940s. Believe it or not, at one point, Hollywood actually understood technology! So think of and thank them every time you use Bluetooth.

Components

Virtually all radios are made up of the same basic elements.

Antennas



Antennas are the way radio signals leave and enter radios. There’s a lot of seemingly magical designs out there -- beautiful and bizarre.

Vertical, Whip, Dipole

Flickr: rvaphotodude

Wikipedia: Zuzu

Wikipedia: Carnildo

The most visibly common kind of antenna is, in essence, a piece of wire whose length is matched to the wavelength of the radio frequencies it's intended to receive. For lower frequencies (30MHz and below), these antennas are often too big to be practical.

Yagi-Uda

Flickr: mikedent

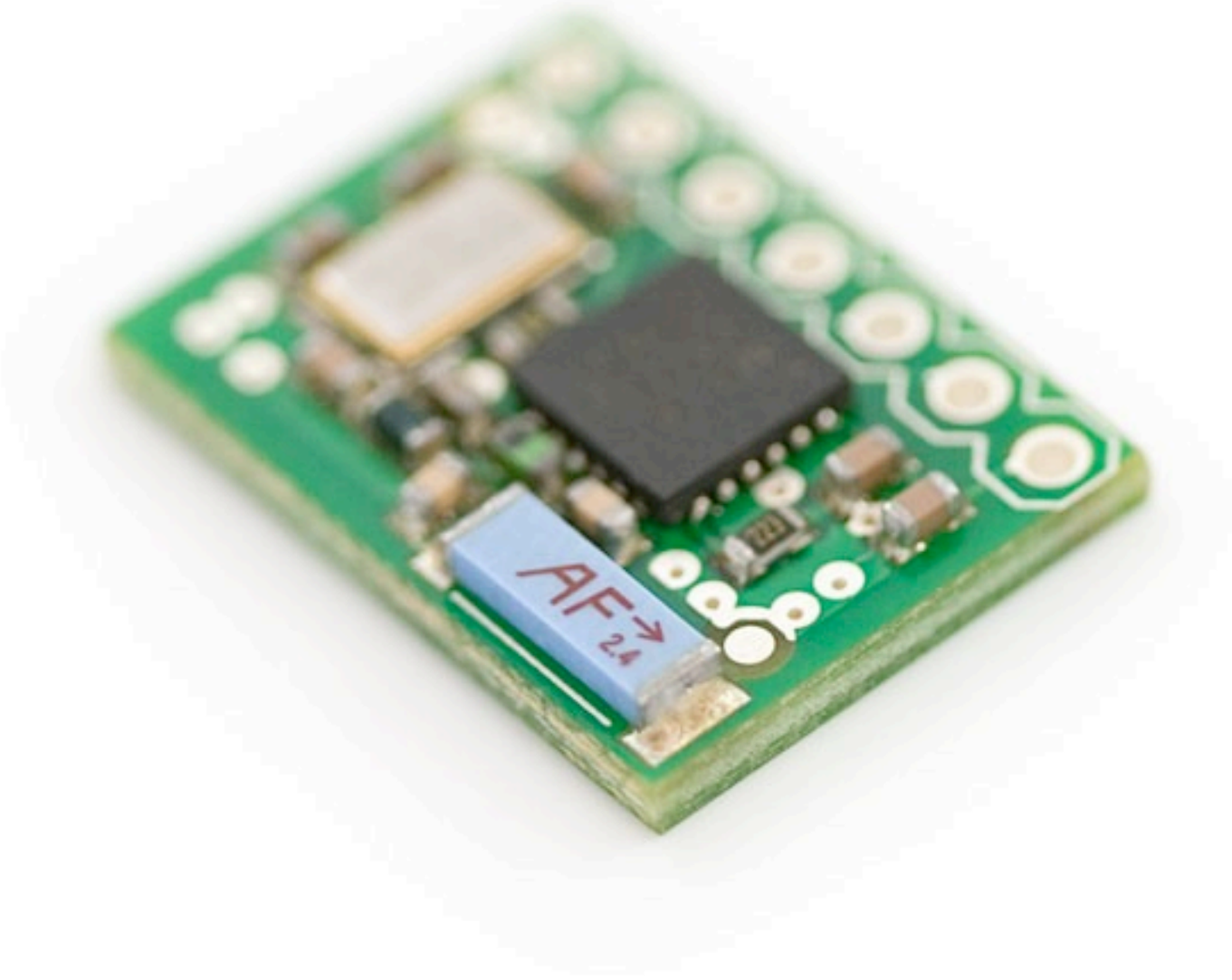
The Yagi builds on the idea of matched lengths by grouping several elements together to increase sensitivity in certain directions (a directional antenna).

Helical

Wikipedia: public domain

Helical antennas are one way to get a long antenna in a smaller space, or produce a very efficient directional antenna -- great for tracking a satellite.

Chip Antenna

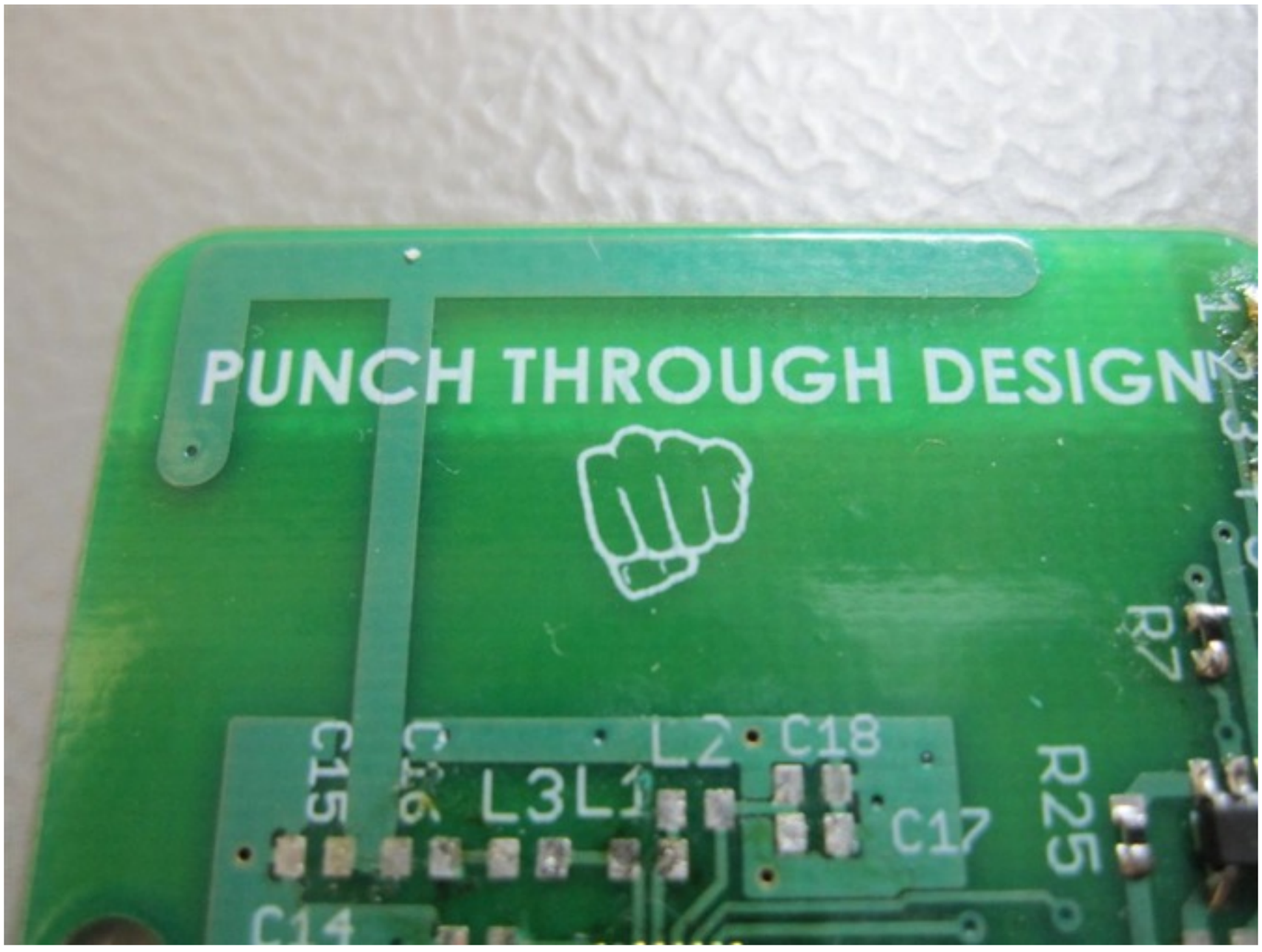


www.creatroninc.com

Wednesday, June 27, 12

Chip antennas (like this little blue part) are only practical at high frequencies where the signal wavelength is small. They fold an antenna into a small package that's suitable for a portable device.

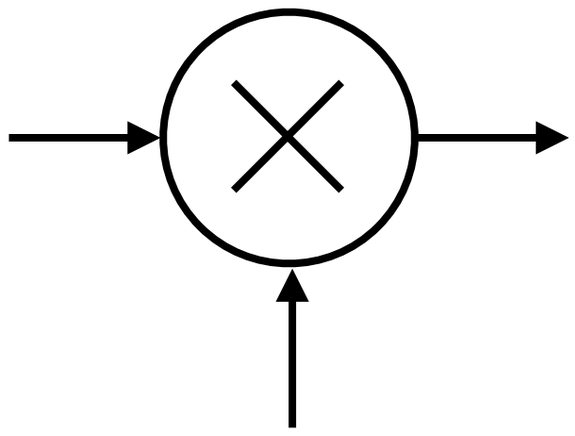
PCB Trace Antenna



http://colinkarpfinger.com/blog/2010/the-dropouts-guide-to-antenna-design/

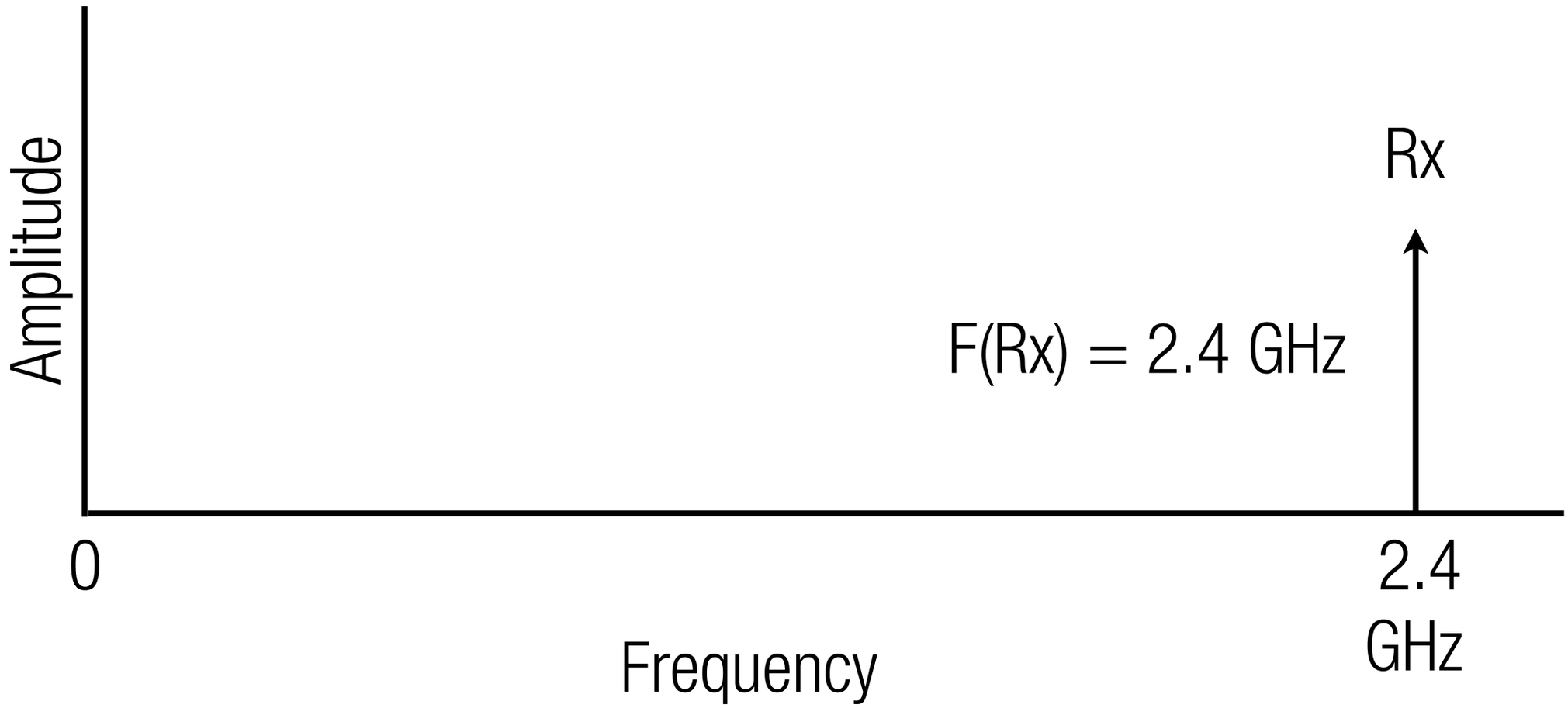
Circuit board antennas are the simplest antenna solution, very common for cheap consumer electronics. When designed correctly, they work fairly well, too. But designing them correctly is not particularly easy... It's very much an iterative process.

Mixers



Mixers in radio are not at all like mixers for audio. A *radio* mixer is used to shift a signal in frequency, to make it easier to process.

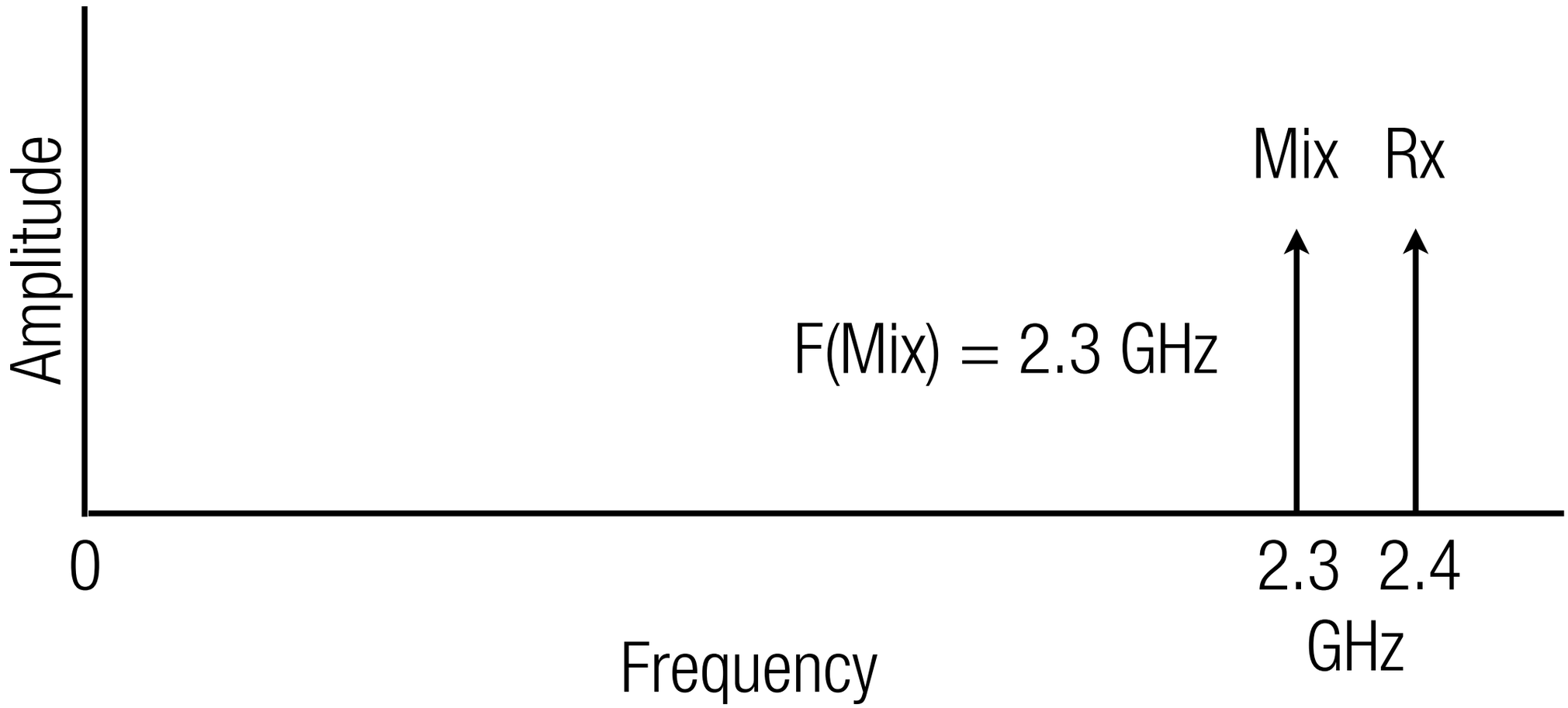
Frequency Translation



Wednesday, June 27, 12

For instance, it’s very hard to design a 2.4 GHz Wi-Fi radio receiver that processes signals at 2.4GHz. Processing signals at 2.4GHz (or even 1GHz) is a challenging design problem for a number of reasons. Instead, radios use mixers to shift the desired signal to another range of frequencies that's easier to work with. Here, we have a signal at 2.4 GHz that we want to shift to a lower frequency for processing.

Frequency Translation



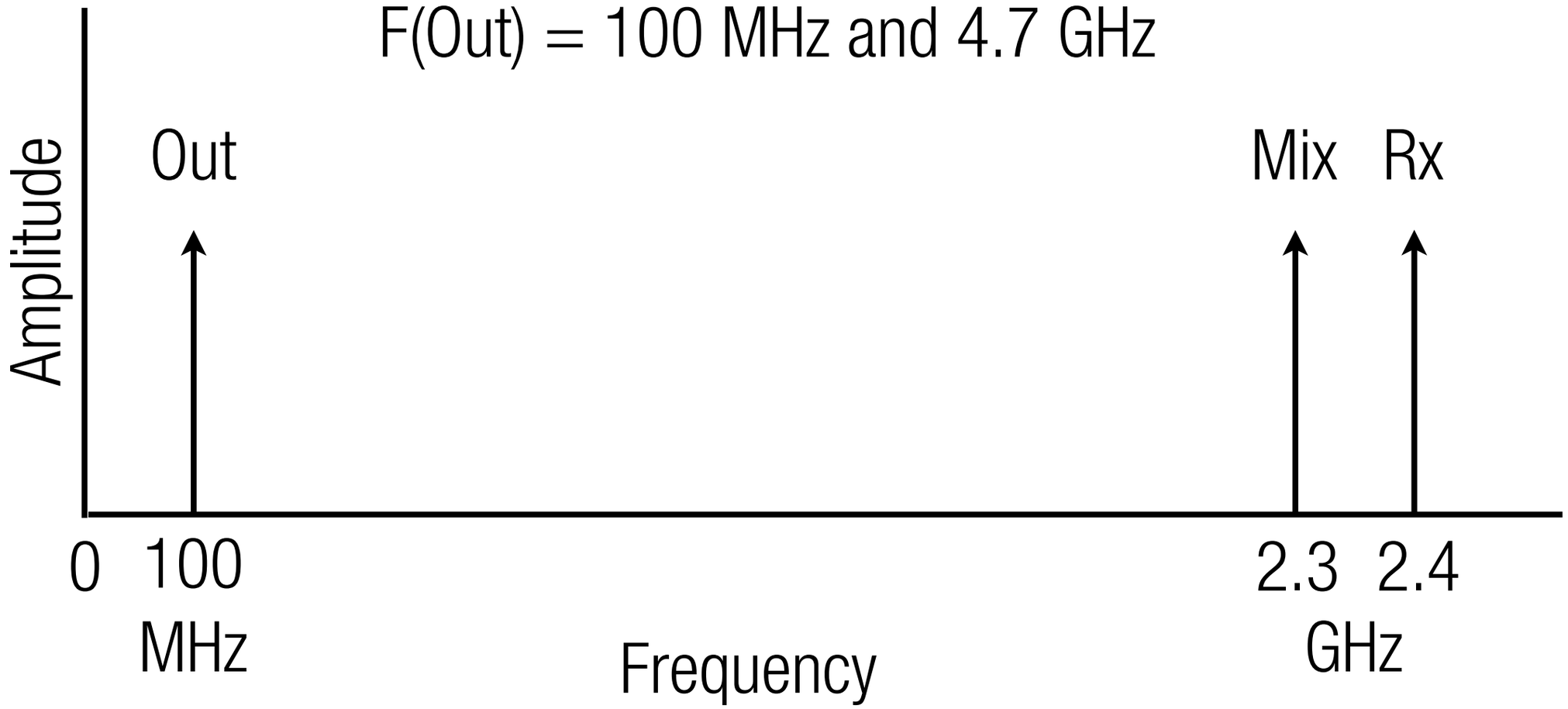
Wednesday, June 27, 12

We'll mix it with a 2.3 GHz signal.

Frequency Translation

F(Out) = F(Rx) +/- F(Mix)

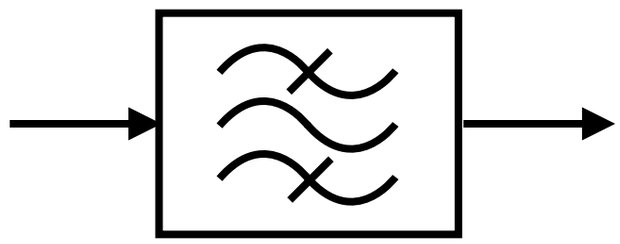
F(Out) = 100 MHz and 4.7 GHz



Wednesday, June 27, 12

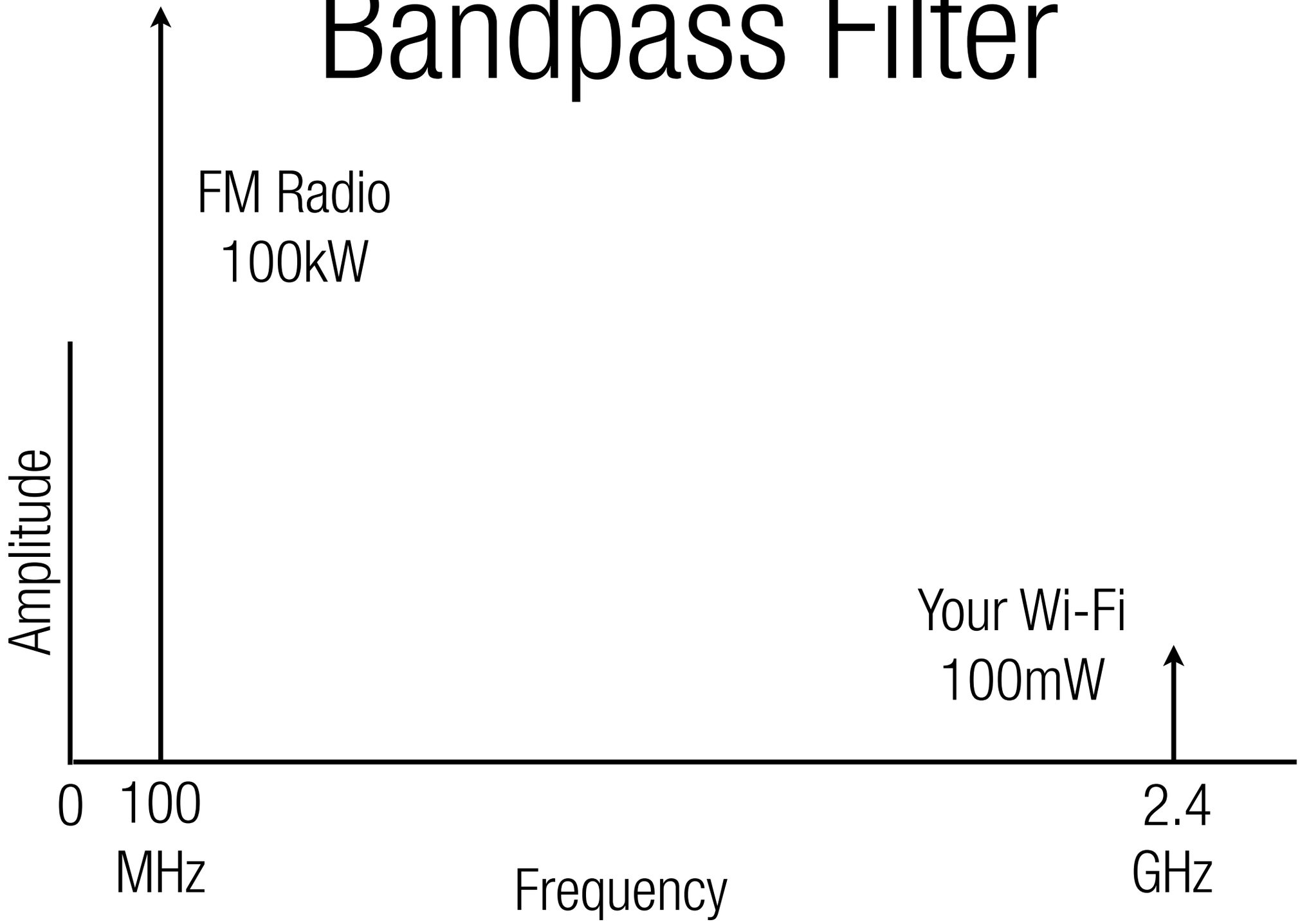
The output of a mixer produces two copies of the signal -- one shifted up by the frequency of the mix signal, and one shifted down by the frequency of the mix signal. So we get two copies of the signal, one at 100 MHz and one at 4.7 GHz (not shown). We can filter out the 4.7 GHz signal, and we're left with just the 100 MHz signal.

Filters



Filters are used to separate desired signals from noise that arises both in the “air” and in the radio circuitry. Antennas pick up noise. Amplifiers produce noise. Mixers produce noise (side effect of the mixing process). Noise is everywhere.

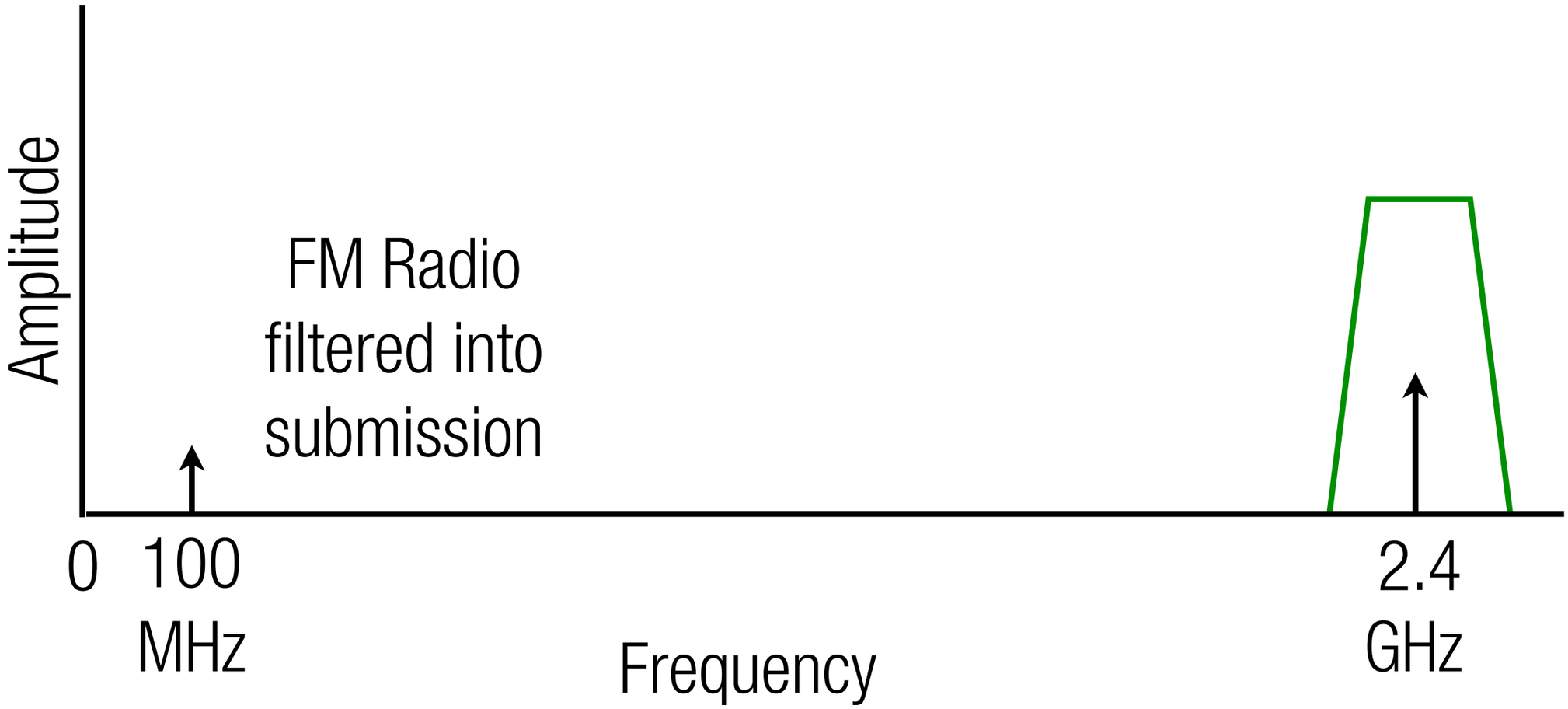
Bandpass Filter



Wednesday, June 27, 12

Consider Wi-Fi. If you live near an FM radio tower, your 100 milliWatt access point is competing with 100,000 Watts of FM broadcast power. True, it's on a completely different frequency, but it can still overload a radio receiver if the radio doesn't filter it out.

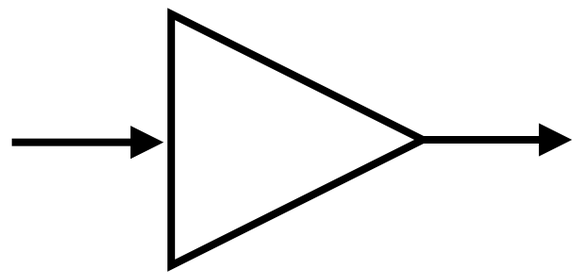
Bandpass Filter



Wednesday, June 27, 12

So a bandpass filter is used inside the receiver. In this case, it filters out everything except the 2.4 GHz band that Wi-Fi operates in. Now, FM radio won't drown out the signal from your access point.

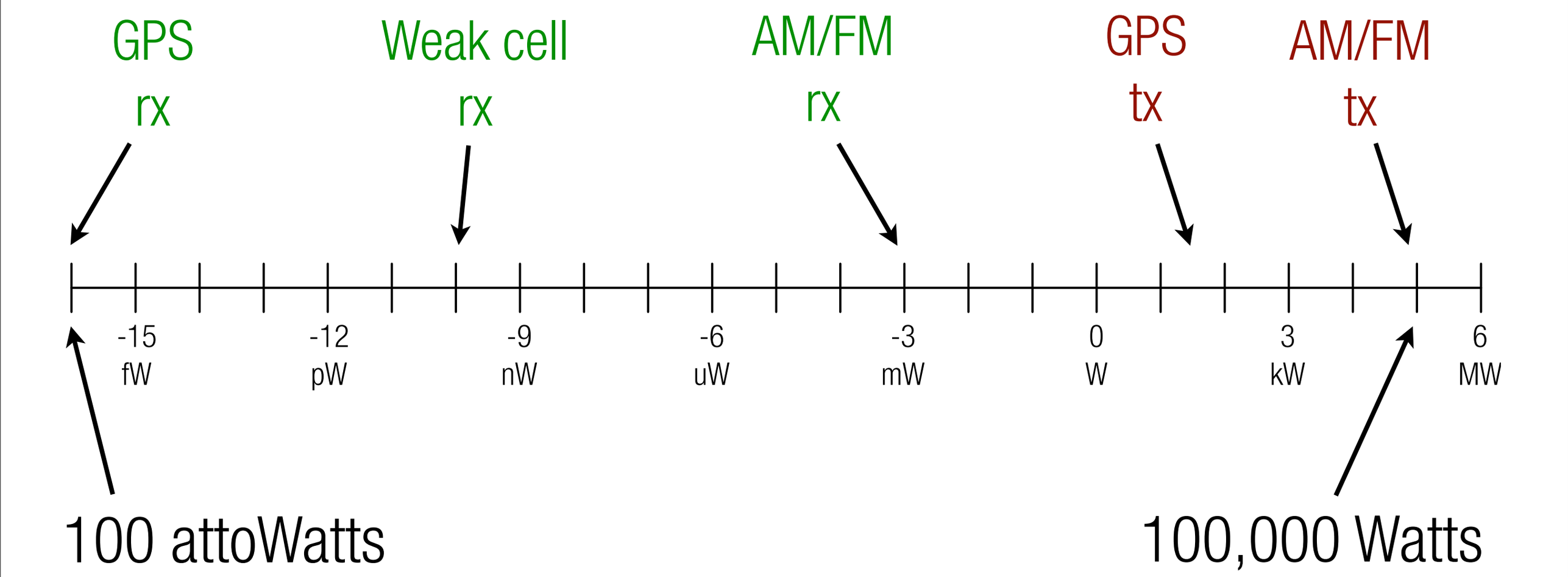
Amplifiers



Amplifiers, no surprise, are used to amplify a signal. The power of a radio signal, at a receiver, is typically very weak, so lots of amplification is necessary.

Signal Power

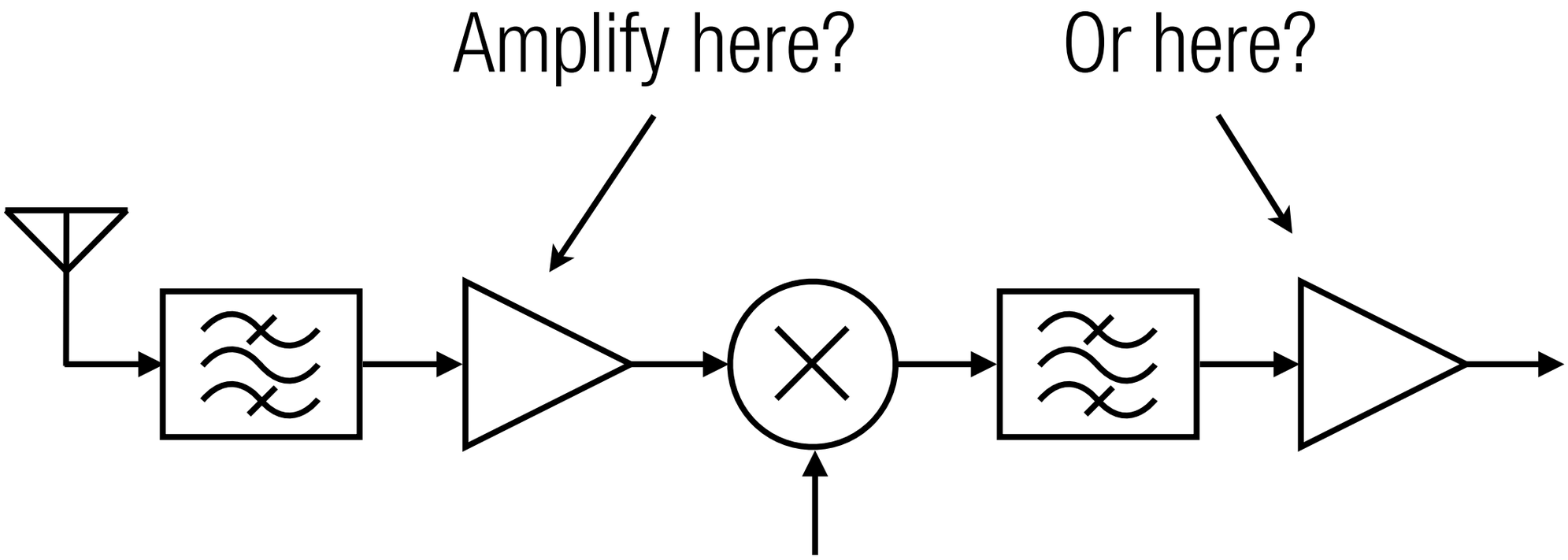
on a log-10 scale



Wednesday, June 27, 12

An extreme example is GPS. GPS satellites are over 20,000 kilometers from Earth. Each satellite transmits only 50W of power -- about one light bulb's worth. Why not more power? There aren't many power plants in space, so there's not much available power for the transmitter to use. That 50W is beamed out over nearly half the Earth. It's spread super-thin -- by the time the signal reaches Earth, a GPS receiver gets roughly 100 attoWatts of power to work with! That's one millionth of a picoWatt. One million-billion times less power than it takes to light up an LED!

Amplify Carefully...



Or both?!

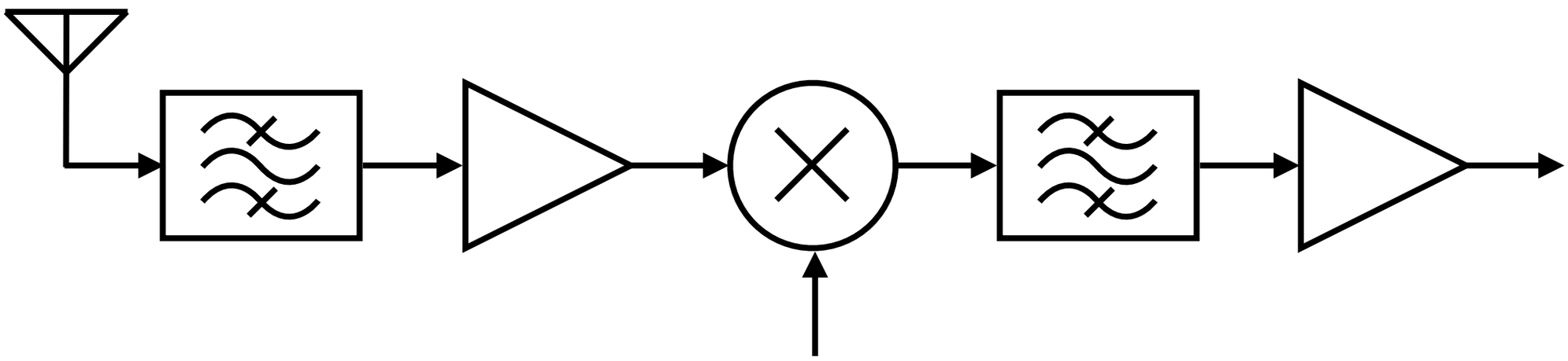
And how much?

So most signals need a lot of amplification to be processed, and to not be swallowed up by the noise internal to the radio receiver. Because of that, there are lots of subtleties around where amplification is done within a radio. Amplification early in the circuit can overcome noise in circuits later in the signal path. But amplify too much and strong signals will overload the radio and distort the desired signal. Bad (low-quality) amplifiers, or the wrong amplifiers, will amplify alright, but add too much noise to the signal and defeat the purpose of amplification.

Digital-ization of Radio

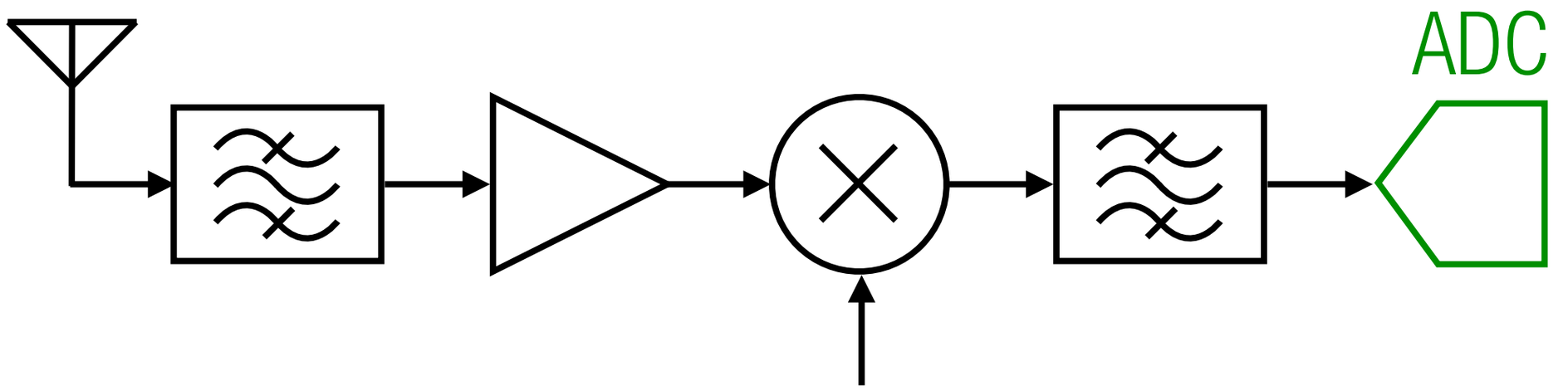
In the last twenty years or so, radio technology has shifted solidly into the digital domain.

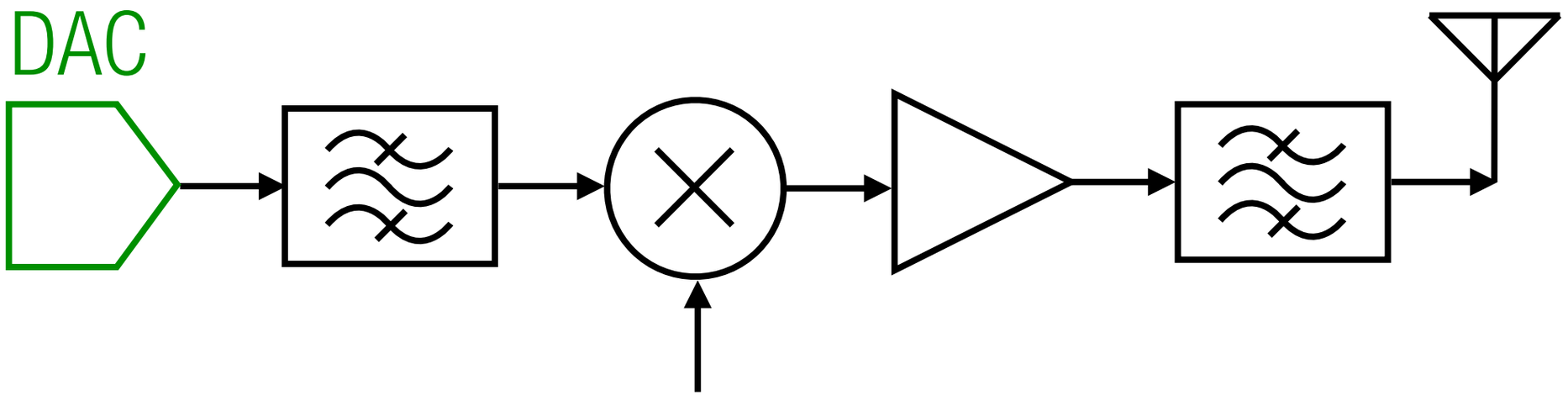
Analog Is Old-Skool



Radios have historically been analog -- modulation, mixing, amplification, filtering, demodulation. Even complex radio devices like televisions worked purely in the analog domain.

Digital Baseband

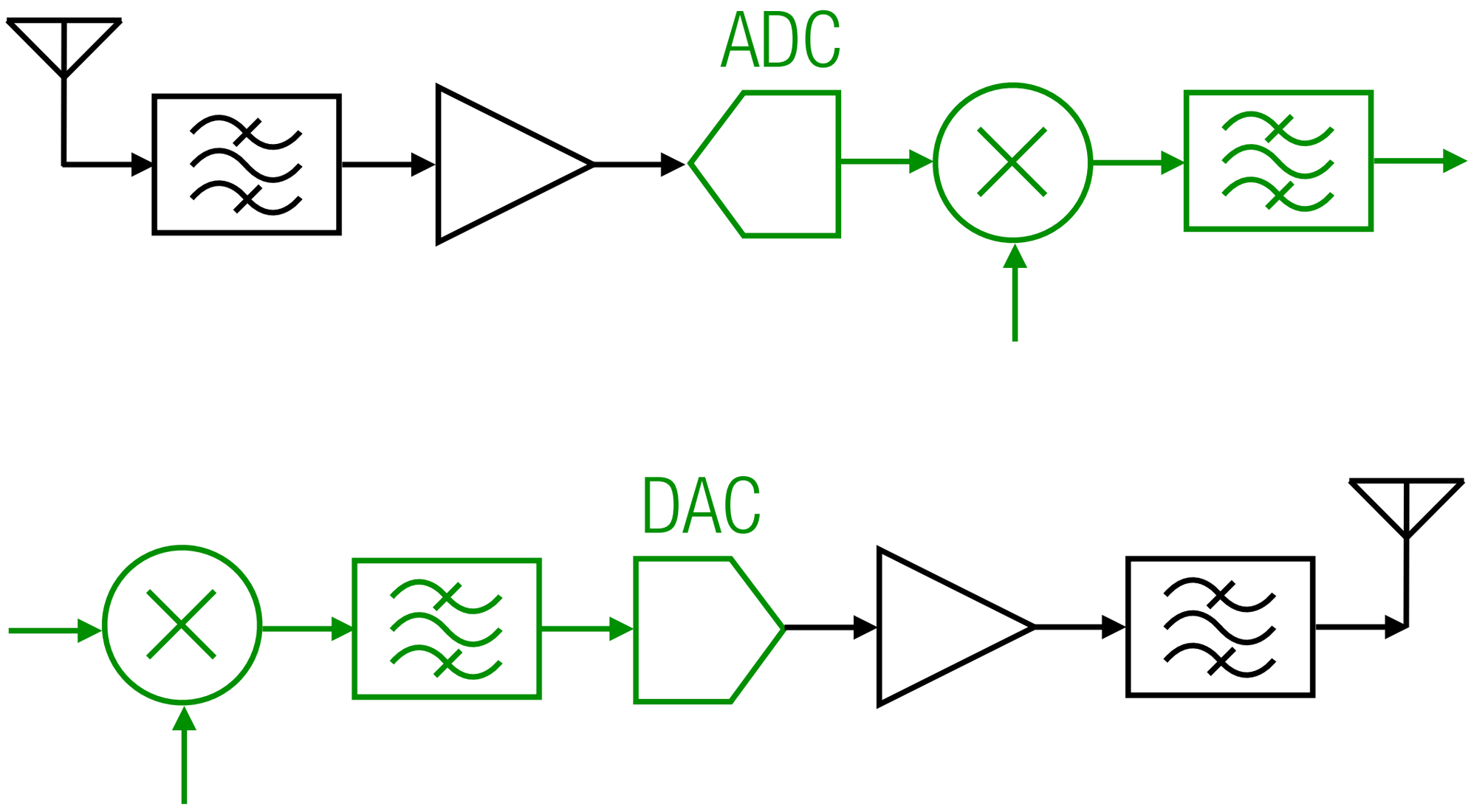




Wednesday, June 27, 12

But, as happened in the 1990s with audio, it's become practical and affordable to digitize radio signals and process them digitally with hardware or software. At first, radios became digital at the “baseband”, or the portion of the radio circuit where the signal is low-frequency. A digital device like a signal processing chip, microcontroller, or full-blown computer performs the modulation and demodulation, instead of analog hardware.

Digital To The Antenna



And just like audio converters in computers progressed from 16 bits to 24 bits resolution, and from 48kHz to 96kHz and 192kHz sampling, radio-frequency converters are progressing toward the point where they can digitize or generate signals directly at the radio carrier frequency. More of the radio can be implemented digitally -- mixing and filtering in particular.

So Why Digital?

- Because everything else is becoming digital.
- Digital enables software, software enables flexibility.
- Digital can do things analog can't (practically).

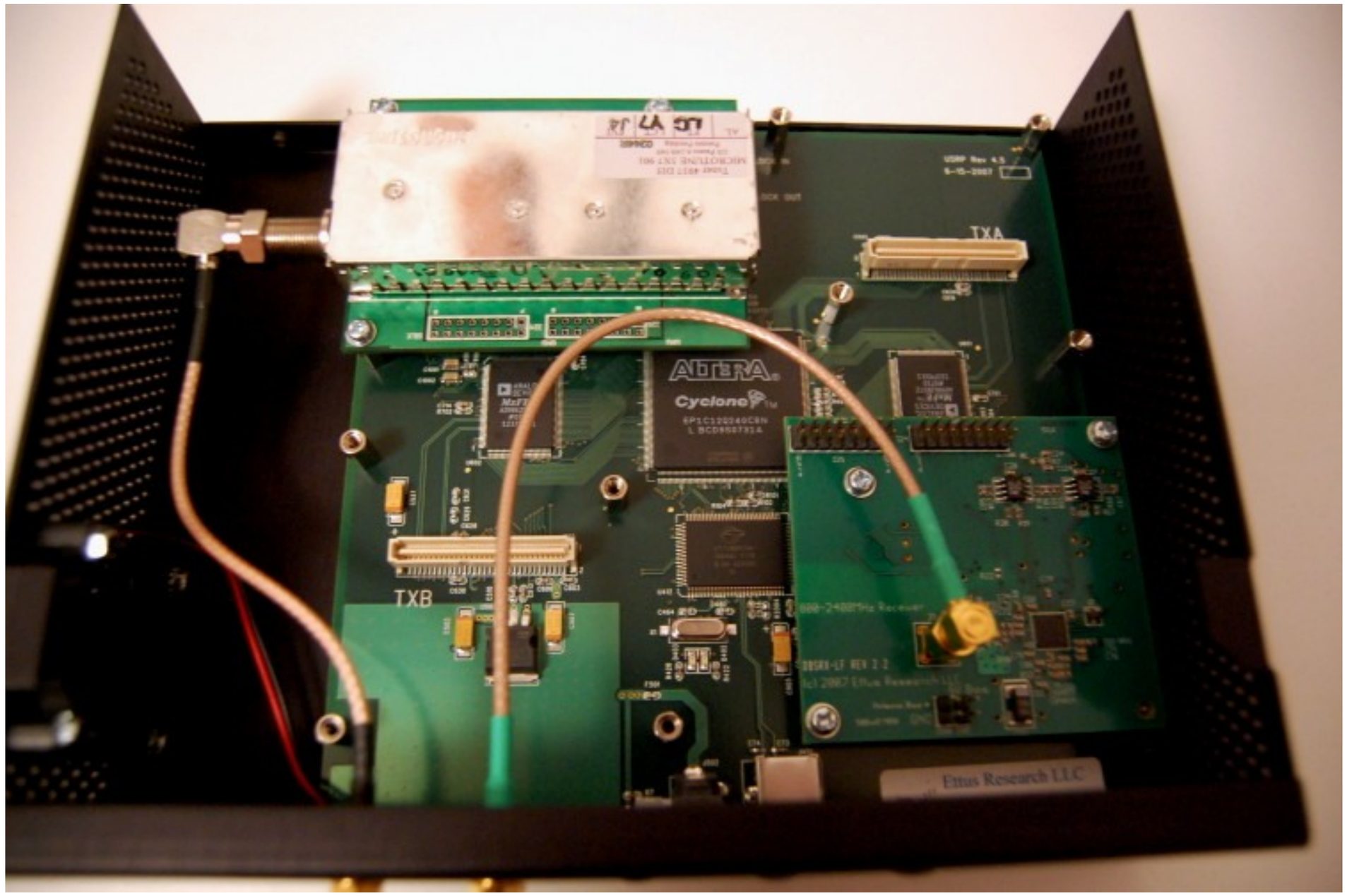
So why would you want a digital radio? Mostly by necessity -- more communication devices are digital these days, as is the information we want to communicate. Digital audio, digital images, digital messages -- it makes sense to transport this digital data in the digital domain. Digital radios also provide the option to do some of the radio processing in software. Software can be upgraded when bugs are discovered or new radio technologies are rolled out. Lastly, modern signal processing techniques can do amazing things, pulling information out of horrible noise and applying error correction to recover lost data. These techniques aren't practical with a purely analog radio.

Hardware

What are some examples of digital radio hardware, that a curious person can use to explore radio signals?

USRP

https://www.ettus.com/product



Flickr: carrierdetect

One of the oldest open-source hardware projects (and products) out there is the USRP (Universal Software Radio Peripheral). It's a very capable device and is used for a lot of radio and security research. But it's on the expensive side, especially for a hobbyist. I happen to have one with me today, loaned to me by a friend.

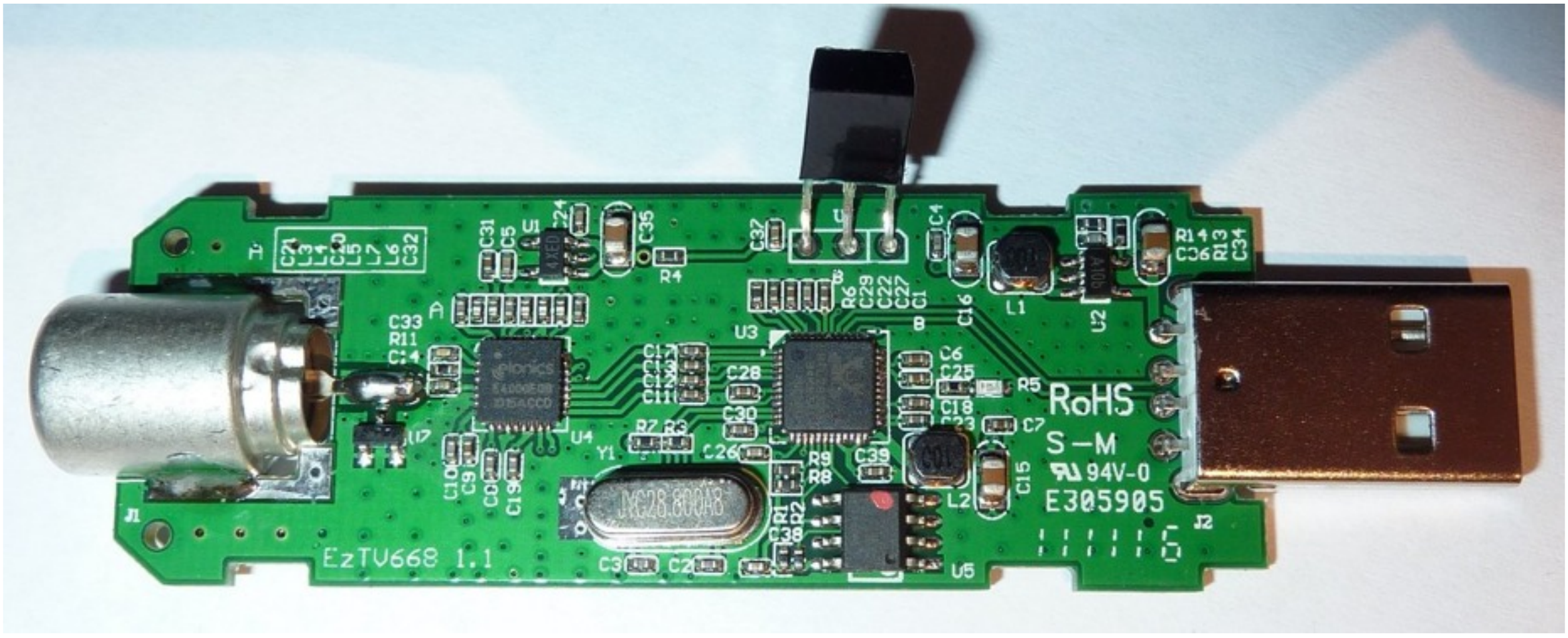
FUNcube Dongle

http://www.funcubedongle.com/

The FUNcube Dongle is very inexpensive, but not particularly open-source. It depends on chips made by manufacturers who will not provide documentation outside of a non-disclosure agreement. But there's good software support for it.

rtl-sdr

http://sdr.osmocom.org/trac/wiki/rtl-sdr

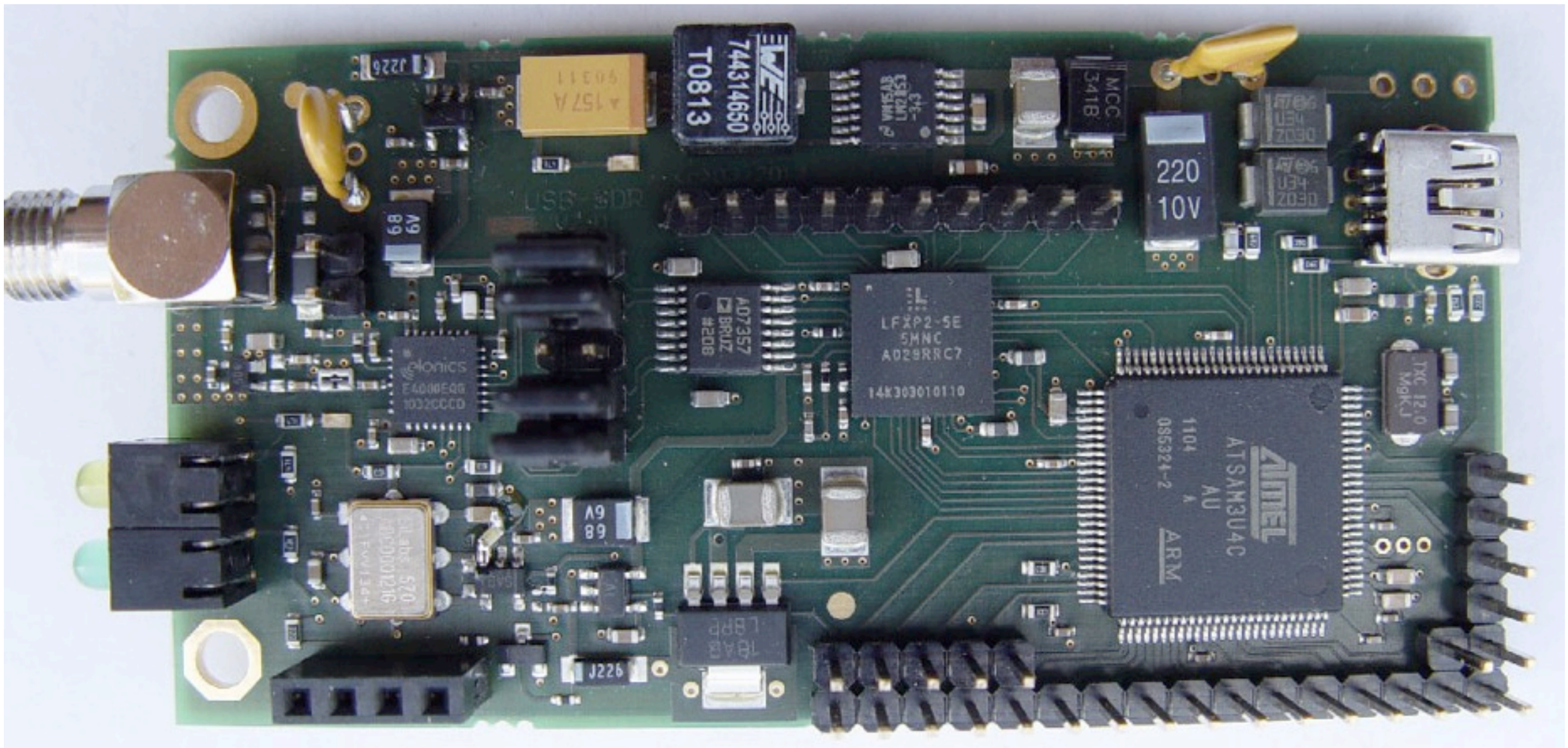


Wednesday, June 27, 12

The rtl-sdr project is building software support for inexpensive DVB-T receiver dongles. Originally designed for terrestrial TV reception in Europe, they can be used over a similar frequency range as the FUNcube Dongle (64MHz to 1.7GHz), but can capture more bandwidth. The dongle hardware is not open-source, but is very inexpensive.

OsmoSDR

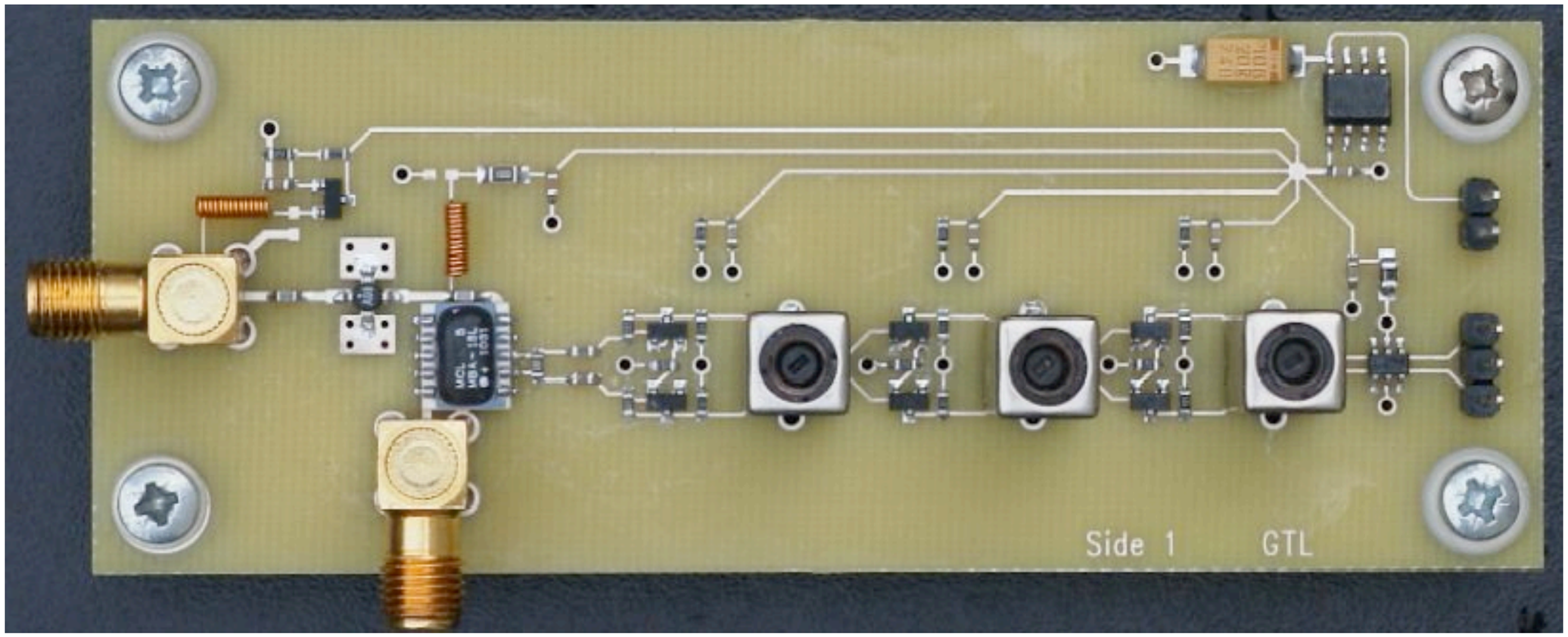
http://sdr.osmocom.org/



The OsmoSDR is similar in design to the rtl-sdr devices, but is more open, higher-quality, and can capture a bit more bandwidth (about 4MHz at a time).

Homemade GPS Receiver

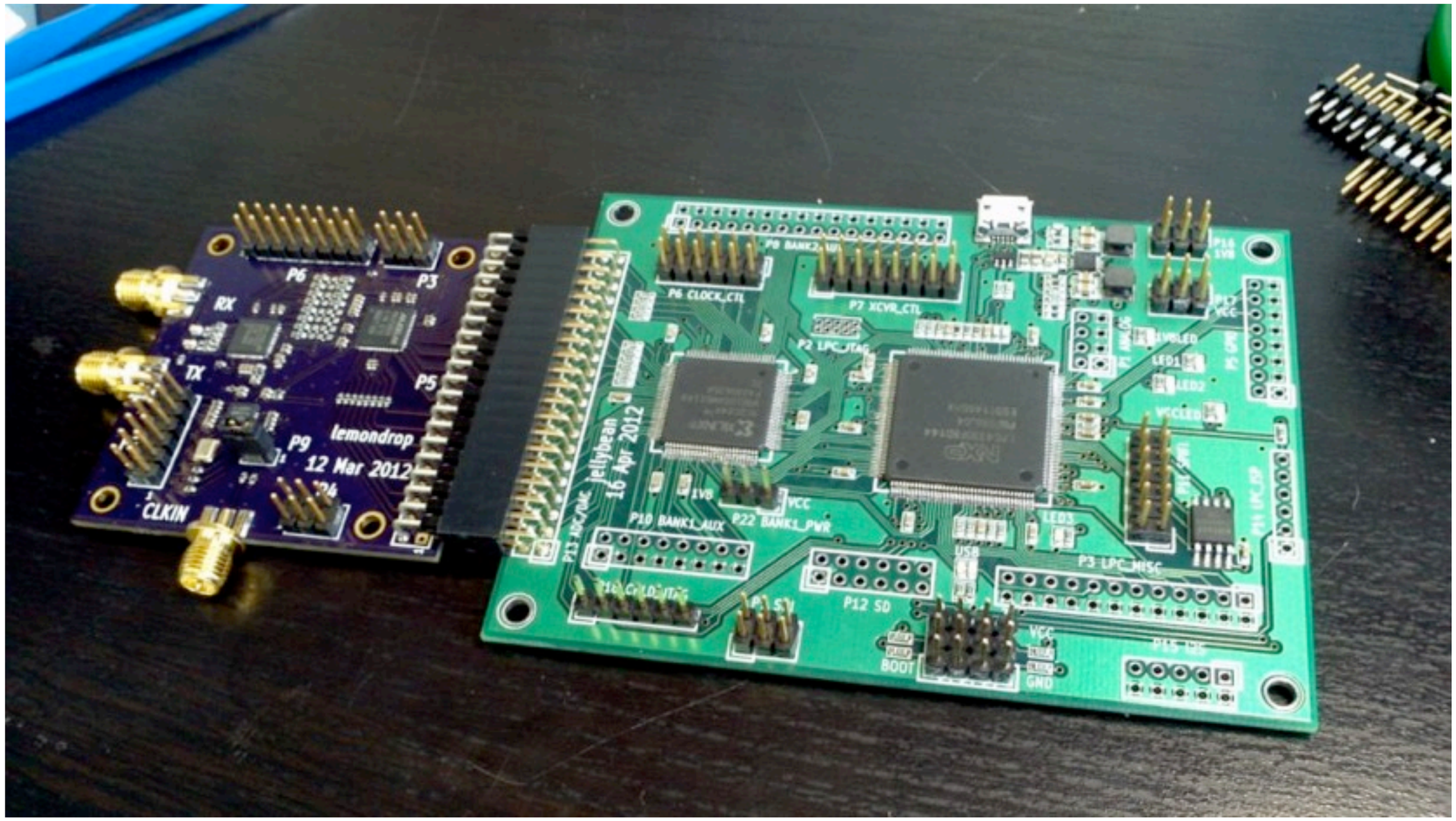
http://www.holmea.demon.co.uk/GPS/Main.htm



This is a one-of-a-kind GPS receiver. It's amazing work by Andrew Holme, built on the work of Matjaz Vidmar. It's a complete receiver, including the RF portion shown above, and a bunch of digital hardware (a field-programmable gate array connected to a PC). His Web page is a wonderful read on how brilliant GPS technology is and how challenging the signals are to work with.

HackRF

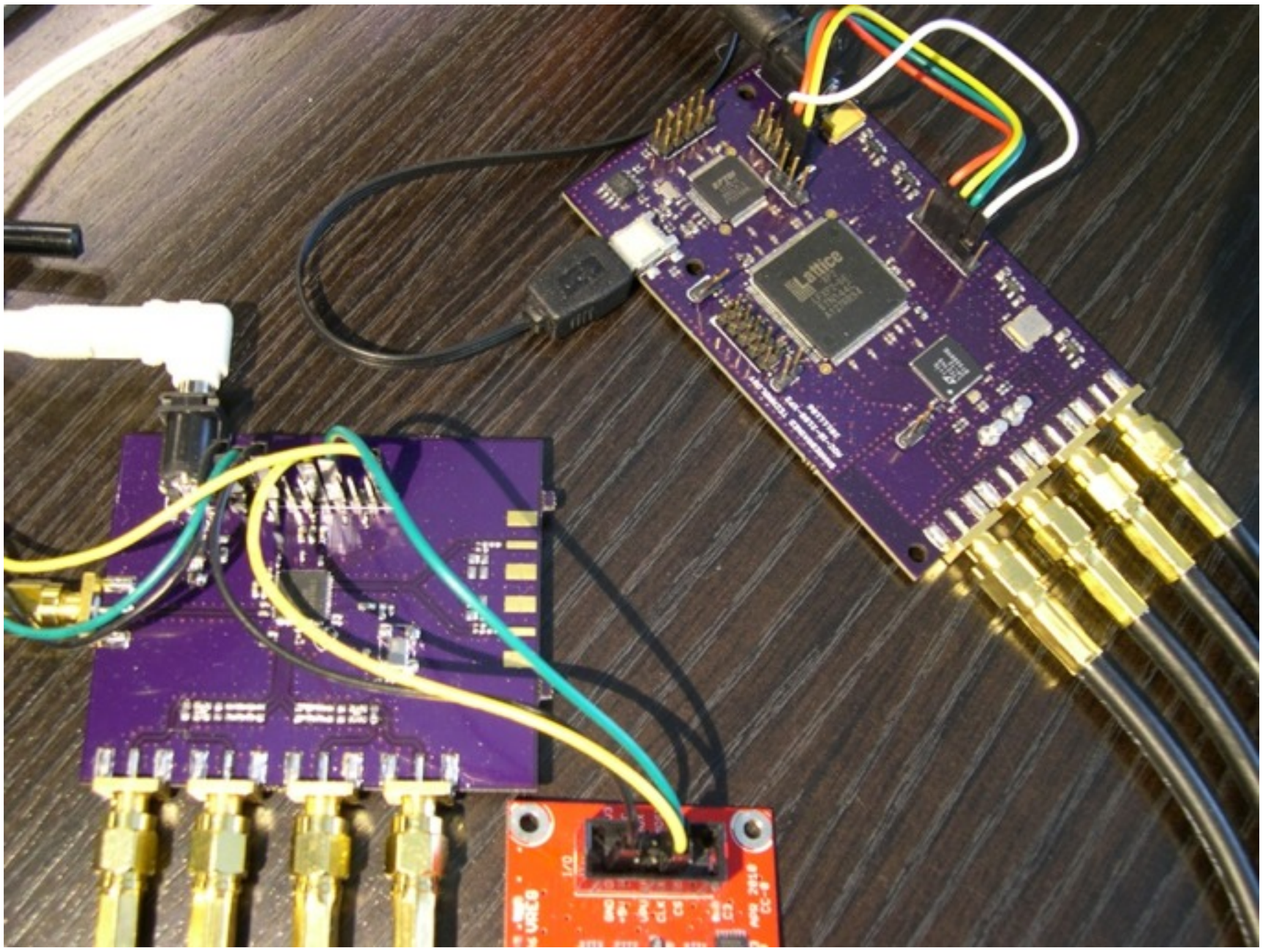
https://github.com/mossmann/hackrf



Michael Ossmann, designer of the Ubertooth One Bluetooth research tool, is developing a wideband radio transceiver, ideally to work from 100MHz to 6GHz. I'm helping him with the project, which is still early in the development process.

My Stuff

https://github.com/sharebrained



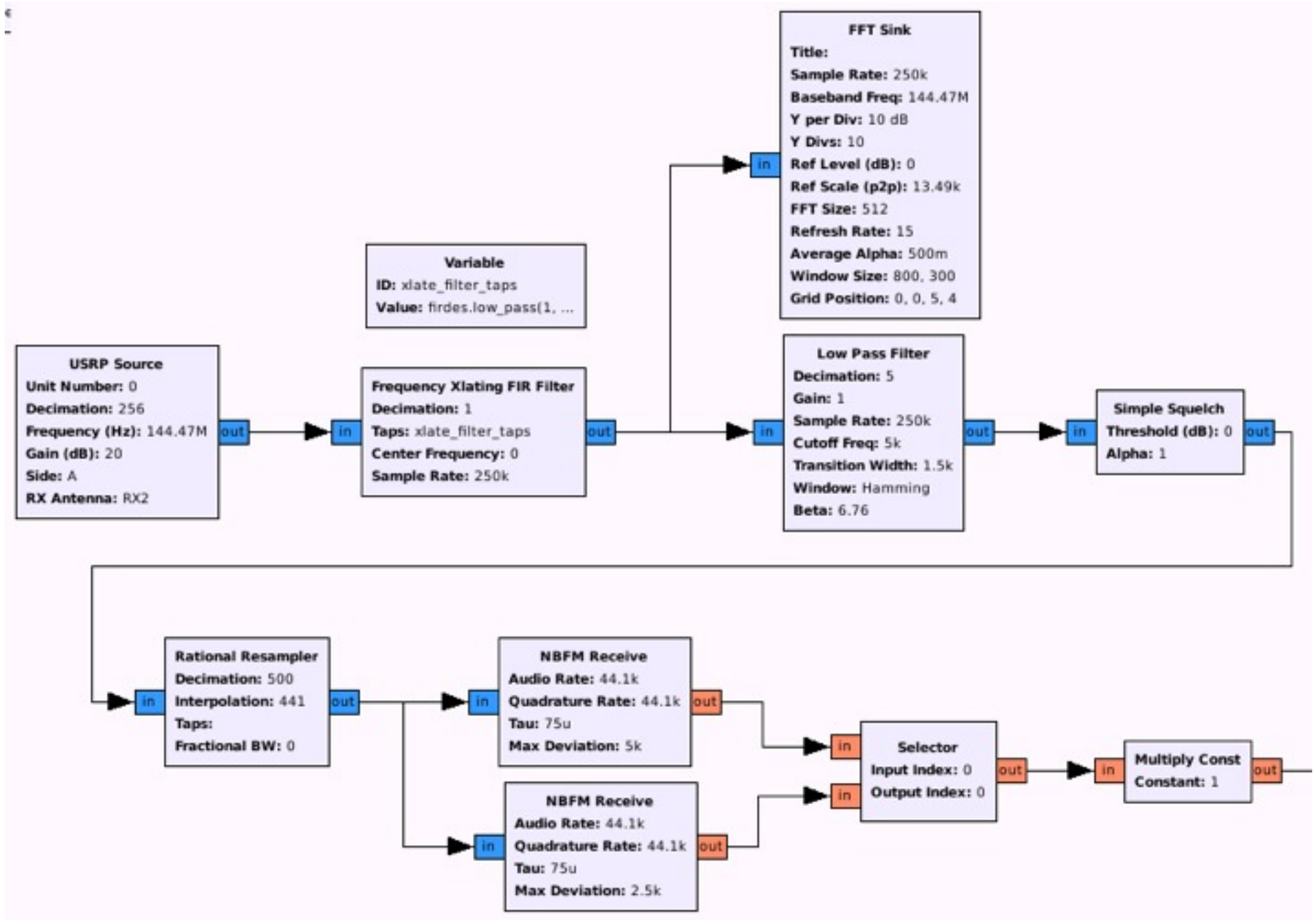
Wednesday, June 27, 12

Last August, I built a 100MHz to 1GHz receiver from an Analog Devices chip. In November, I got a baseband digitizer that can capture up to 8MHz of spectrum at a time, and send it over USB 2.0 high-speed to a PC for processing.

Software

GNU Radio

http://gnuradio.org/



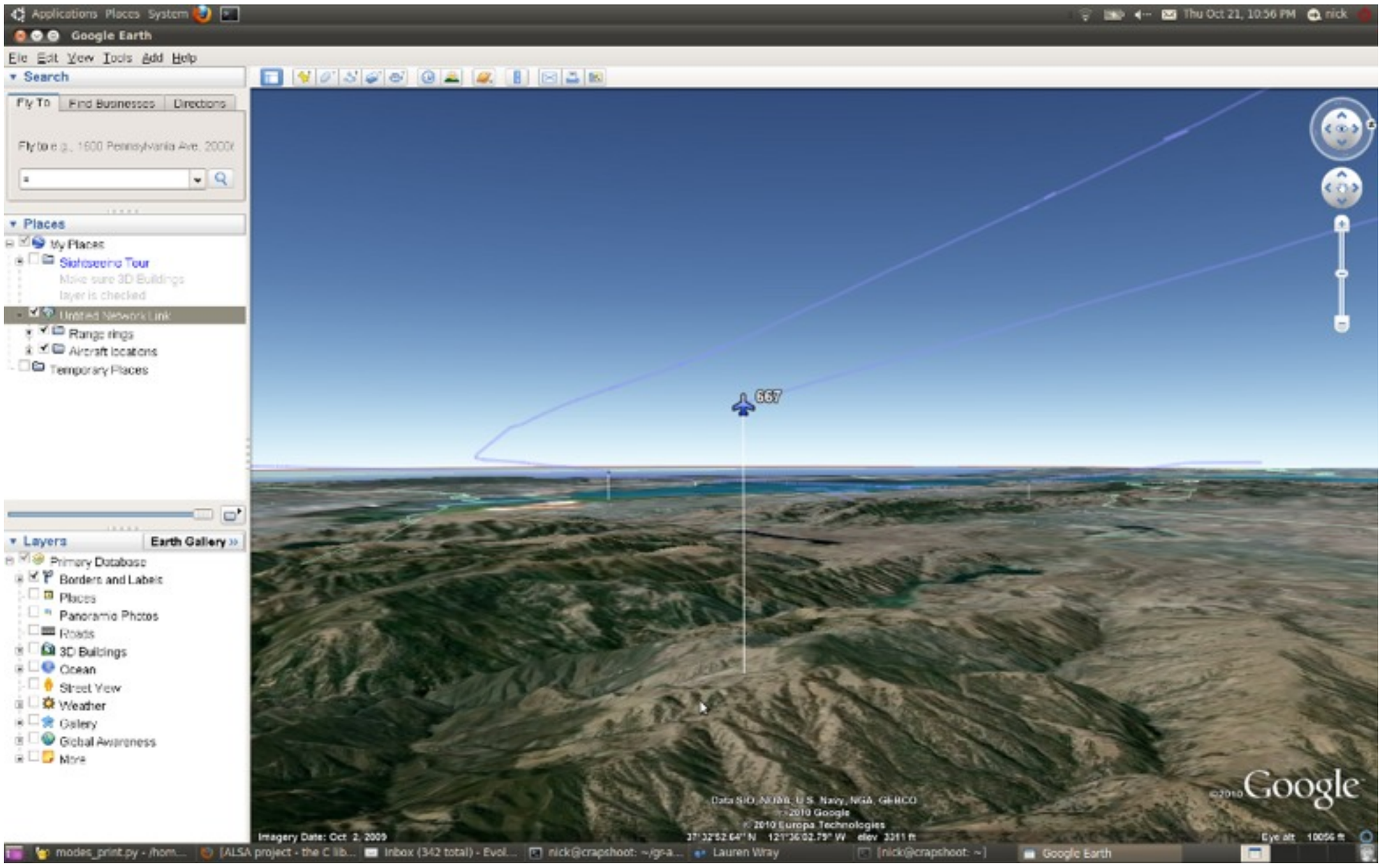
Alexandru Csete

Wednesday, June 27, 12

Perhaps the grandest of all open-source software radio suites is GNU Radio. It's been around for about a decade and is quite advanced. It even has a graphical editor which you can use to create flow graphs of algorithms for processing and generating radio signals. This is the software I use the most, and am most familiar with.

Airplanes!

https://www.cgran.org/wiki/gr-air-modes



Wednesday, June 27, 12

One particularly sexy example of what you can do in GNU Radio is receiving transponder signals from aircraft. Yes, you can do this online, but that's *online*. With a radio, you can receive the signals yourself, directly from the airplane.

Airplanes!

https://www.cgran.org/wiki/gr-air-modes

Raw output from “uhd_modes”:

```
Type 0 (short A-A surveillance) from a01616 at 1100ft
Type 4 (short surveillance altitude reply) from a01612 at 1100ft
Type 0 (short A-A surveillance) from a3c5ea at 12375ft
---
Type 0 (short A-A surveillance) from aa8af8 at 1000ft
Type 0 (short A-A surveillance) from aa8af8 at 900ft
Type 0 (short A-A surveillance) from aa8af8 at 600ft
```


Run “rx-mode-s”.

Here’s some data I pulled out of thin air last night. I live fairly close to the airport, and whenever one of the little Horizon or FedEx planes lands, they go right over my house. You can see a few different planes here. The last four lines clearly show a plane descending to land, from 1,000 feet down to 600 feet.

ICAO 24 Address

http://www.airframes.org/

Looking up “a01616”...

Registration	Manuf.	Model	Type	c/n	l/t	Selcal	ICAO24	Reg / Opr	built	test reg	delivery	prev.reg	until	next reg	status	
N1041L	Cessna	208B	C208	208B0337	L1T		A01616	ATLANTIC AERO INC	1993		1997-05-20				active	edit

And “a3c5ea”...

Registration	Manuf.	Model	Type	c/n	l/n	l/t	ICAO24	Selcal	Reg / Opr	built	test reg	delivery	prev.reg	until	next reg	status	
N342NB	Airbus	A-319-114	A319	1746		L2J	A3C5EA	AMBL	DAL [DL] Delta Air Lines	2002	D-AVYA	2008-10-29	N342NB			active	edit
N342NB	Airbus	A-319-114	A319	1746		L2J	A3C5EA	AMBL	NWA [NW] Northwest Airlines	2002	D-AVYA	2002-05-30		2008	N342NB	to other opr	edit

And “aa8af8”...

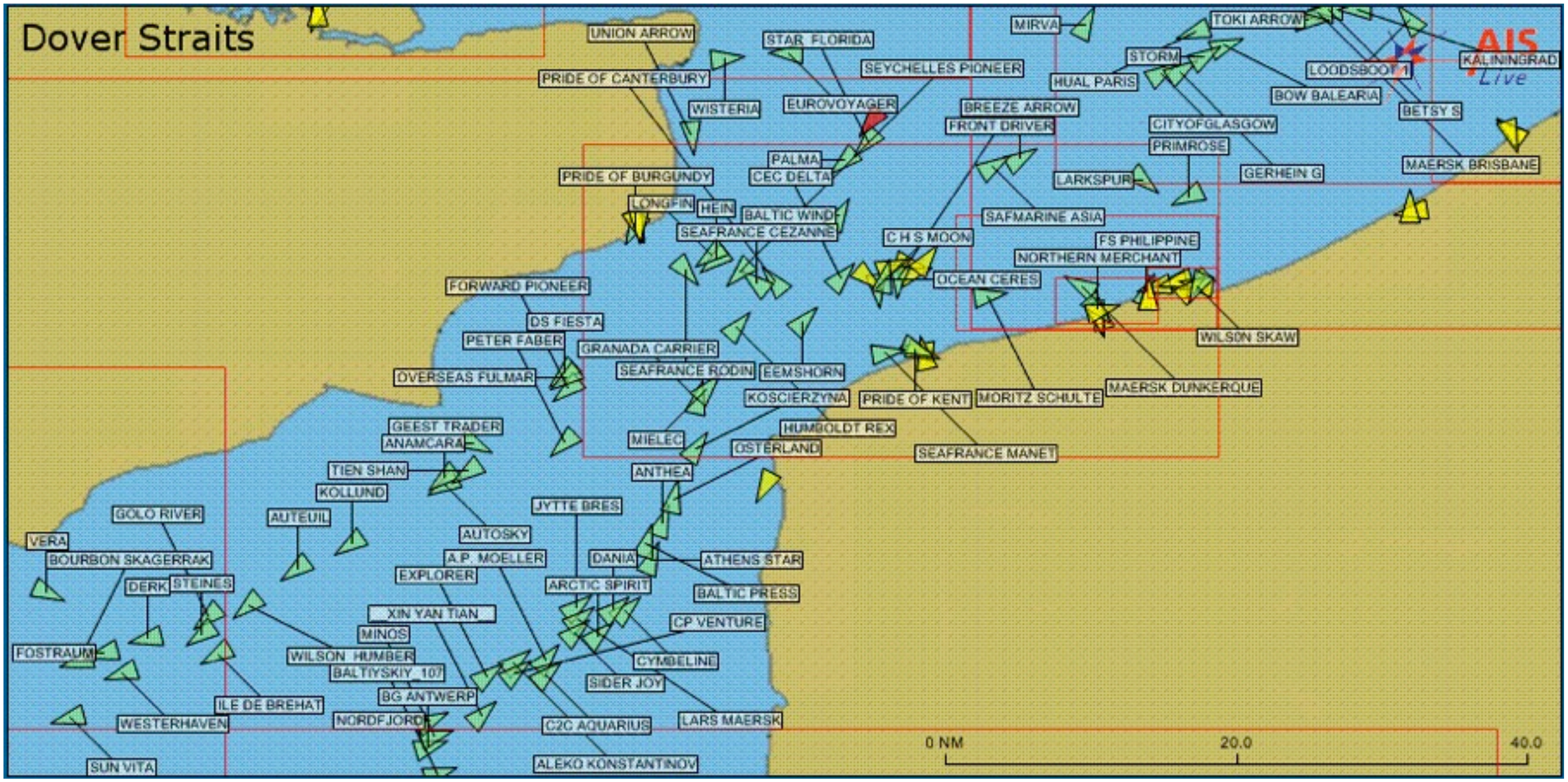
Registration	Manuf.	Model	Type	c/n	l/t	Selcal	ICAO24	Reg / Opr	built	test reg	delivery	prev.reg	until	next reg	status	
N779FE	Cessna	208B	C208	208B0276	L1T		AA8AF8	FEDERAL EXPRESS CORP	1991		1991-08-21				active	edit

Wednesday, June 27, 12

Sure enough, the plane at 1,100 feet over my house is a Cessna 208B. And the plane at 12,375 feet is an Airbus A319. Too cool.

Boats!

https://www.cgran.org/wiki/AIS

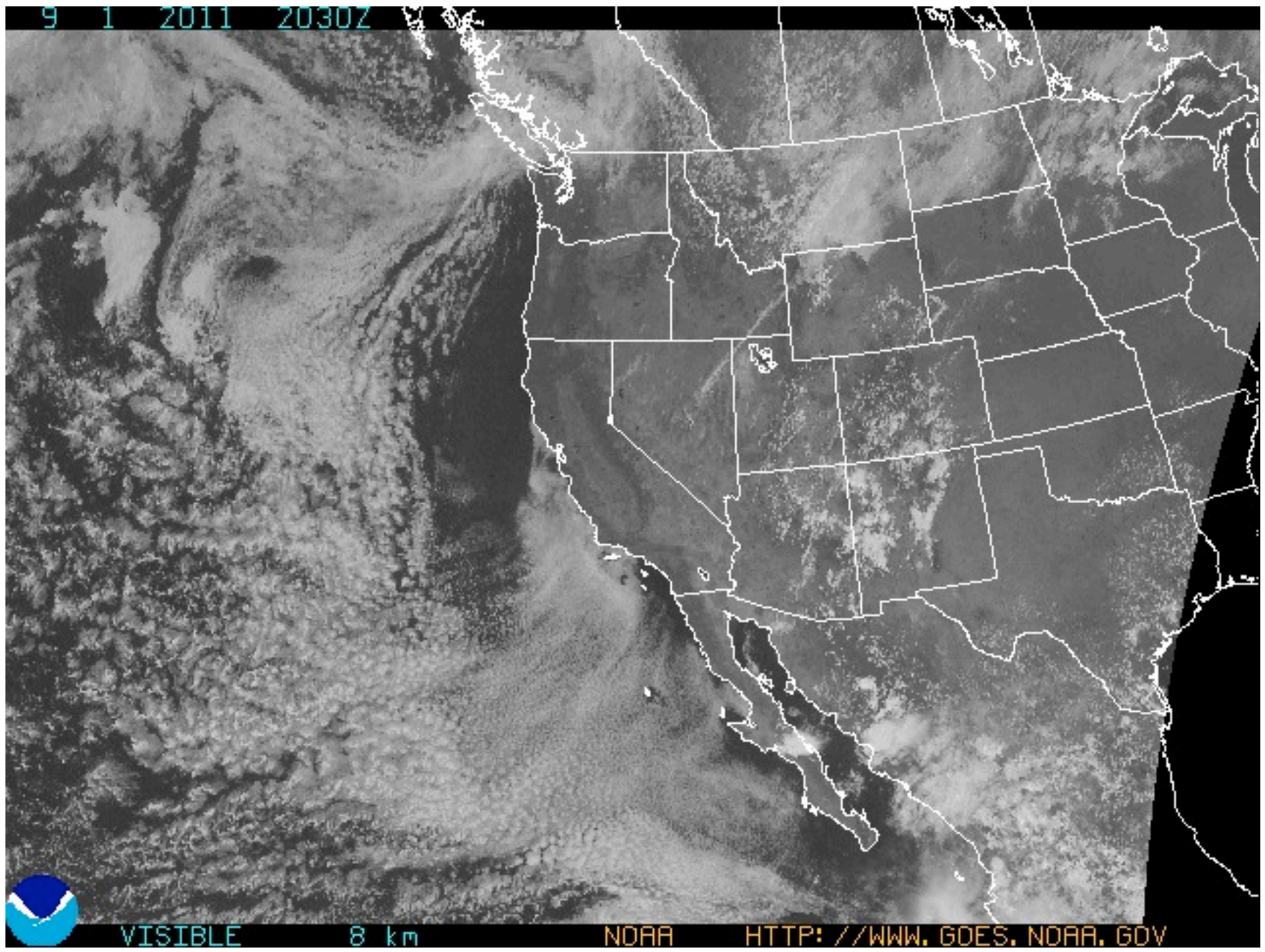


Wikipedia: Pline

Wednesday, June 27, 12

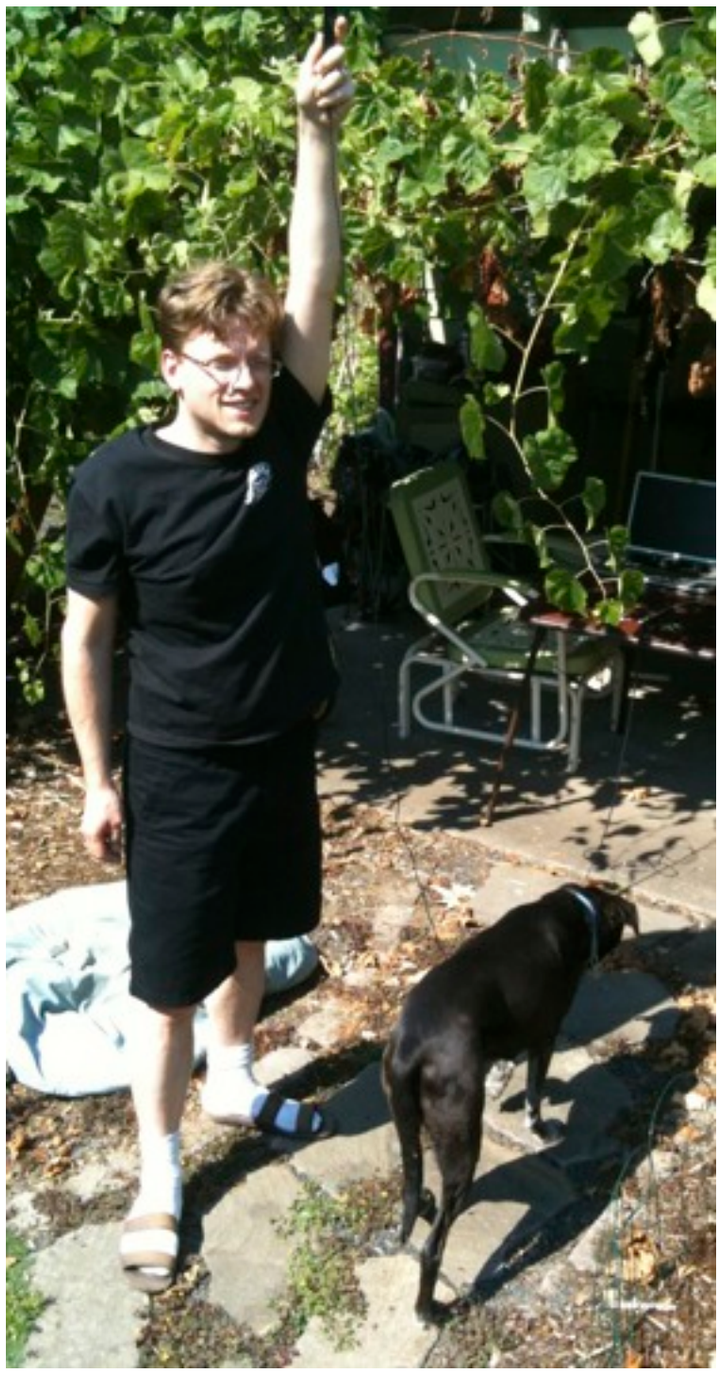
AIS, or Automatic Identification System, is used by boats to communicate their positions.

Satellites!



Some satellites generate signals that can be received and decoded by the public. Here's an image that's probably familiar to you. It's from a National Oceanographic and Atmospheric Administration (NOAA) satellite named GOES. It transmits images that it captures using a very simple modulation scheme.

Satellites!

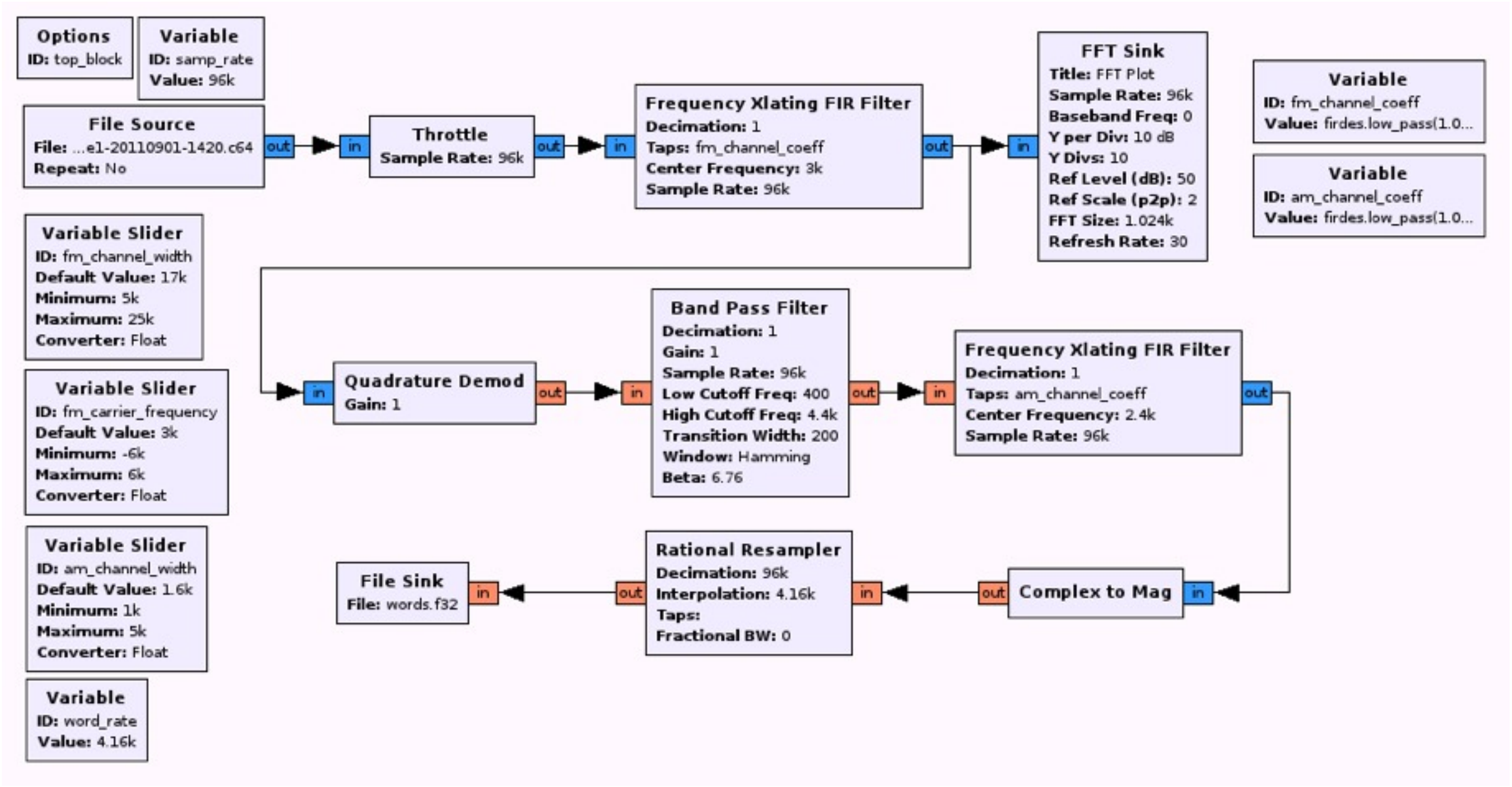


One nice September day, I decided I'd try using my little ADRF6850 receiver board to receive the GOES satellite imagery. Here I am with my cheap Icom antenna, and my laptop in the background, capturing the raw radio signal to disk.

Satellites!

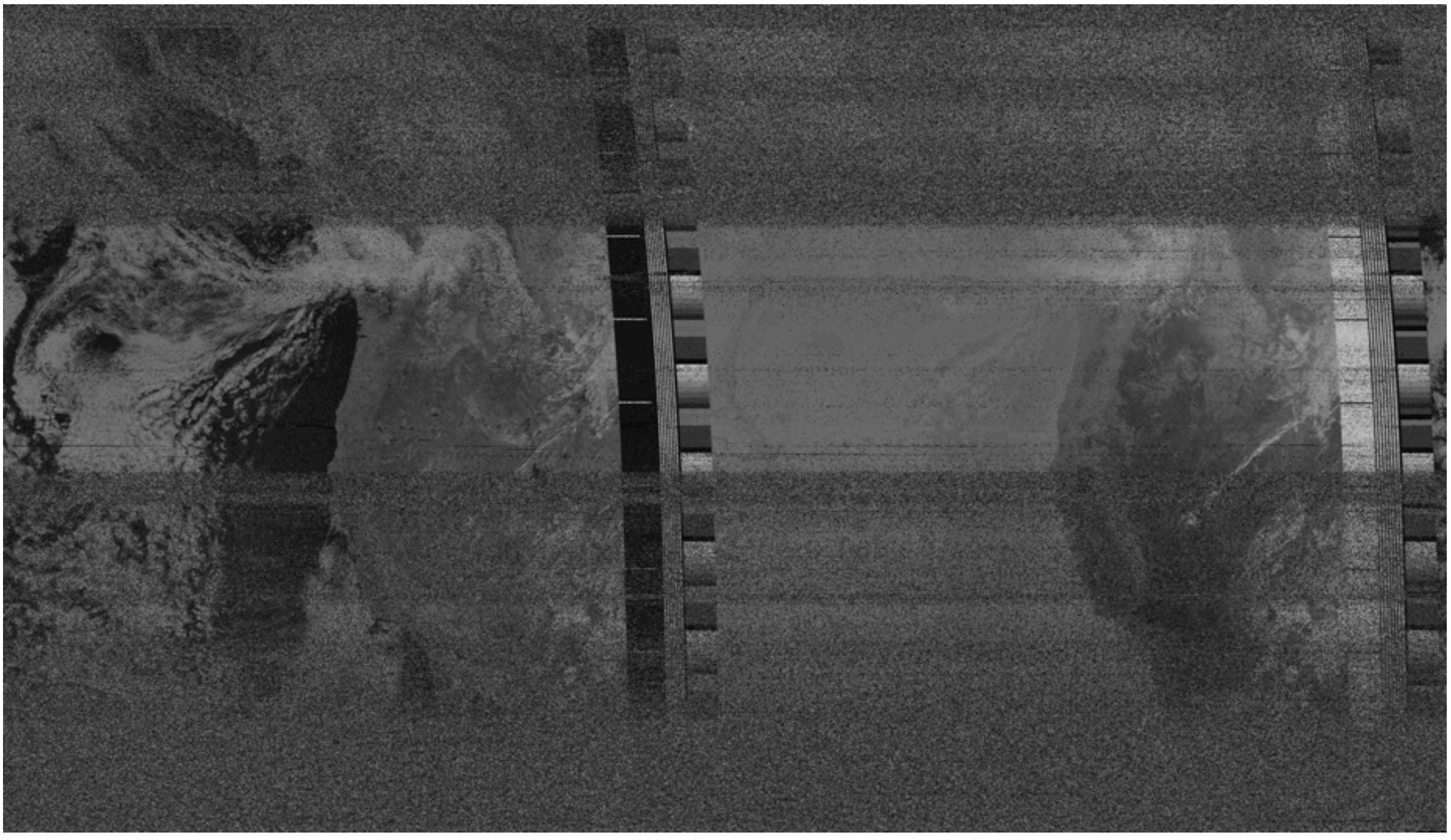
Here’s what I captured, graphed over time. You can hear the frequency of the signal shift as the satellite passes overhead, at roughly 22,000 kilometers an hour. This effect is similar to the Doppler shift when an ambulance speeds by.

Satellites!



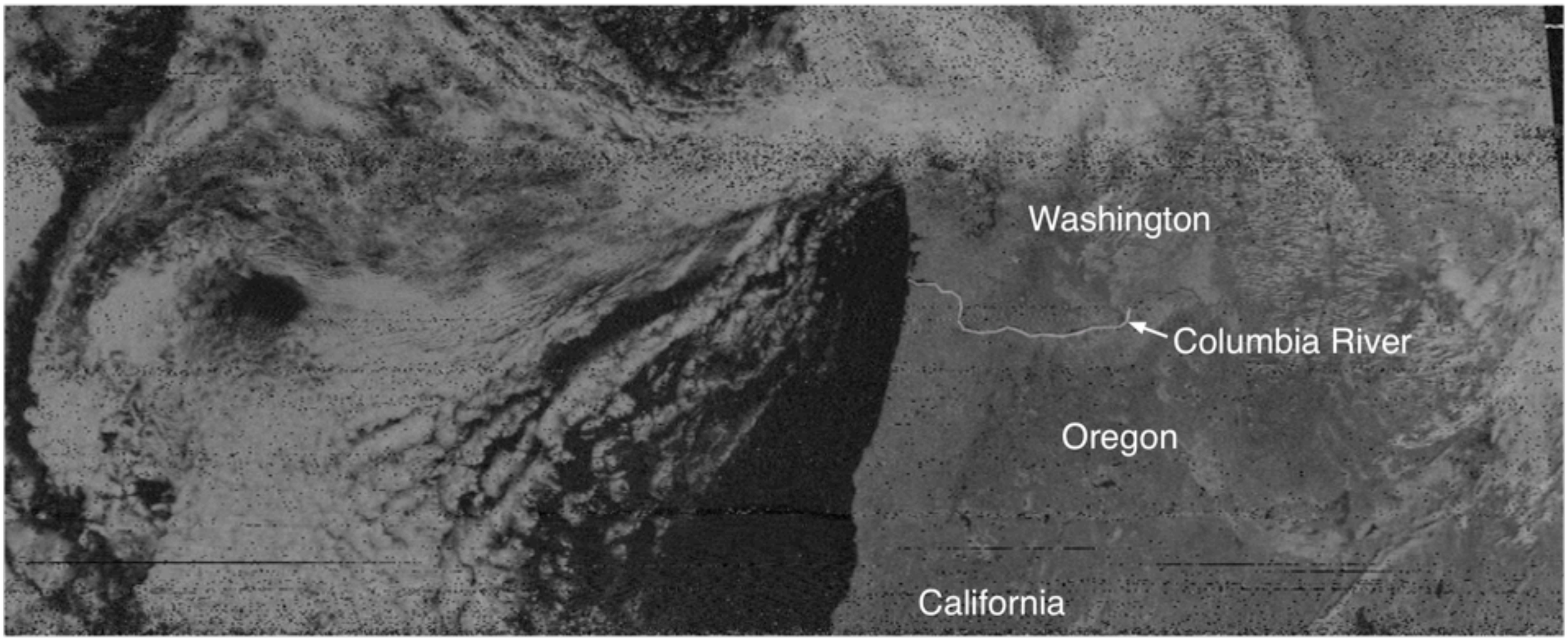
I took the captured file and processed it with GNU Radio, using this algorithm. It writes out a sequence of raw pixel values which I brought into a paint program.

Satellites!



The result looks like this. Kinda nasty, but not bad considering my poor antenna and hardware. With a better antenna and good input filtering on my radio, this picture would be much clearer.

Satellites!



Zooming in, you can see it was fairly nice weather that day!

Demos!

Thanks!