SparkFun Electronics

Nike+iPod Dissection

by Nate | January 13, 2007 | *12 comments* Skill Level: Intermediate

Don't people buy things just to destroy them for self-educational purposes? No? Oh... Well here is another breakdown of the internals of a commercial device. You can learn a lot from professionally engineered devices. Hunting for pictures online of the internals of the Nike+iPod pieces were surprisingly dissatisfying. The only set of pictures available were horribly out of focus, so here is a quick set of pictures to show you how the popular Nike+iPod product works.

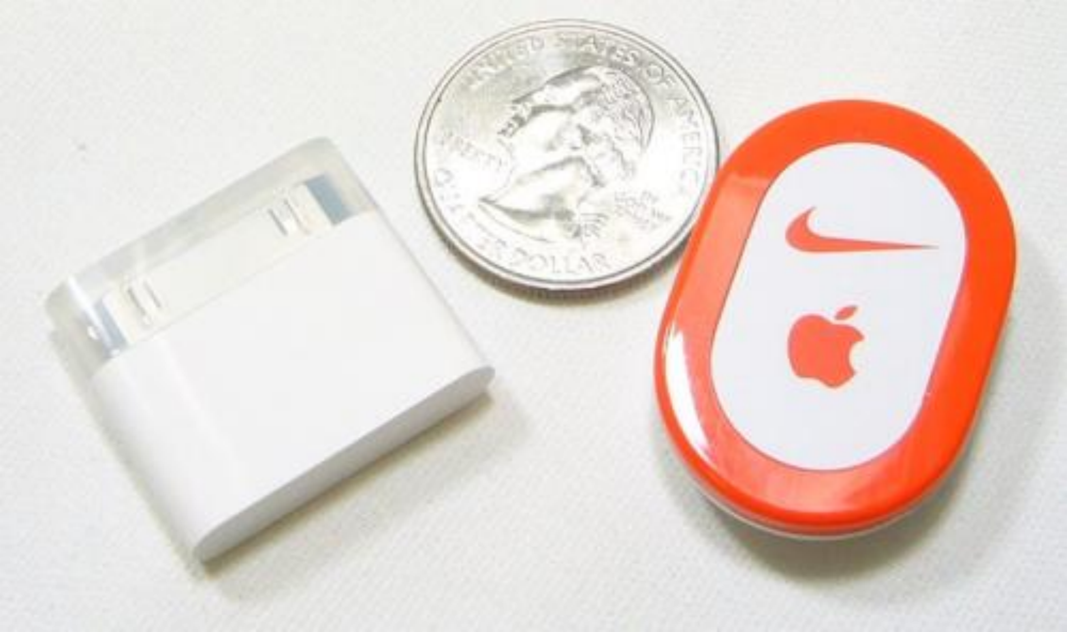
There is a very interesting paper published by some students at U-Dub in the CS department. They basically tapped into the serial connection on the receiver and figured out how to listen for different foot tags. Not surprisingly the news has harped on this as a 'security and privacy risk'. A malicious person *could* design a system to listen for specific tags, as a means of tracking people and places (think crazy ex-boyfriend stalker), but it's just as plausible that we could use this commercially available product (CHEAP! $23.15 internet purchase at time of writing) to monitor where my Grandpa is sleeping, where my 4-year old nephew is playing, or I could automatically turn on/off my lights when I enter my office. Where RFID requires you to physically get near a reader, this active foot pod can transmit over 10-20ft. You don't need to think about getting an RFID card out of your wallet, you just let your shoes do the talking.

The Nike+iPod is not RFID or any form of RFID (Radio Frequency Identification) much to the chagrin of news reporters. While the foot pod does transmit a unique ID, it transmits this information actively in the 2.4GHz band. The foot pod transmits a 'hello world I am XYZ' in very short bursts (less than 0.0001 second per broadcast) on one of 80 available channels every time the user takes a step. This active signal can travel as far as 40-60ft (we don't really care to test the range). The publicly available RFID tags operate in the 125kHz or the 13MHz band and are often passive (requiring the tag to be within a few inches of a RFID 'reader'). The Nike+iPod technology is very different from true RFID systems.

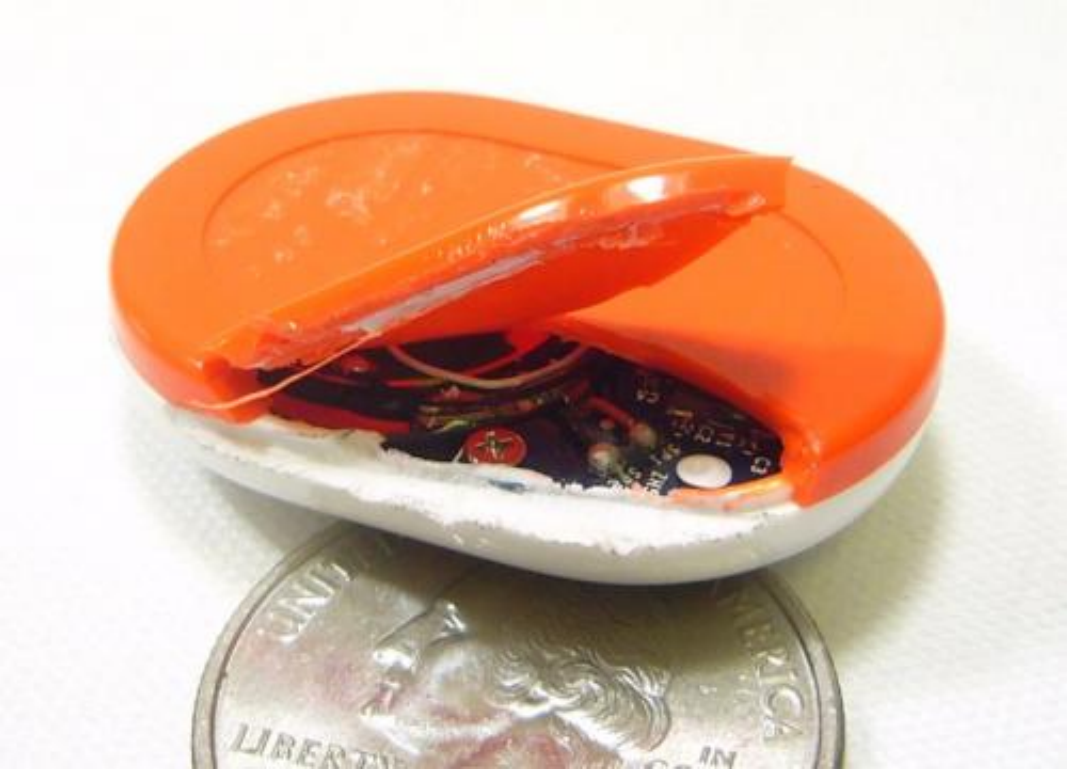
There is no MEMs accelerometer! The foot pod was designed to activate a simple piezoelectric sensor to monitor how long your weight is on the foot (the faster you run, the shorter amount of time spent on one foot). This sensor fires an interrupt within a PIC 16F688 (yea! a PIC microcontroller!). I thought there was going to be an accelerometer built in, but this simpler method reduces the device cost considerably ($8-$10 retail dollars) and probably avoids some nasty patent infringements! Companies like Dynastream and PhatRat (hey, they're just down the street from SparkFun!) use an accelerometer associated with a human's gait and movement to determine overall distance, speed, etc.

Enough! Here are the pictures...

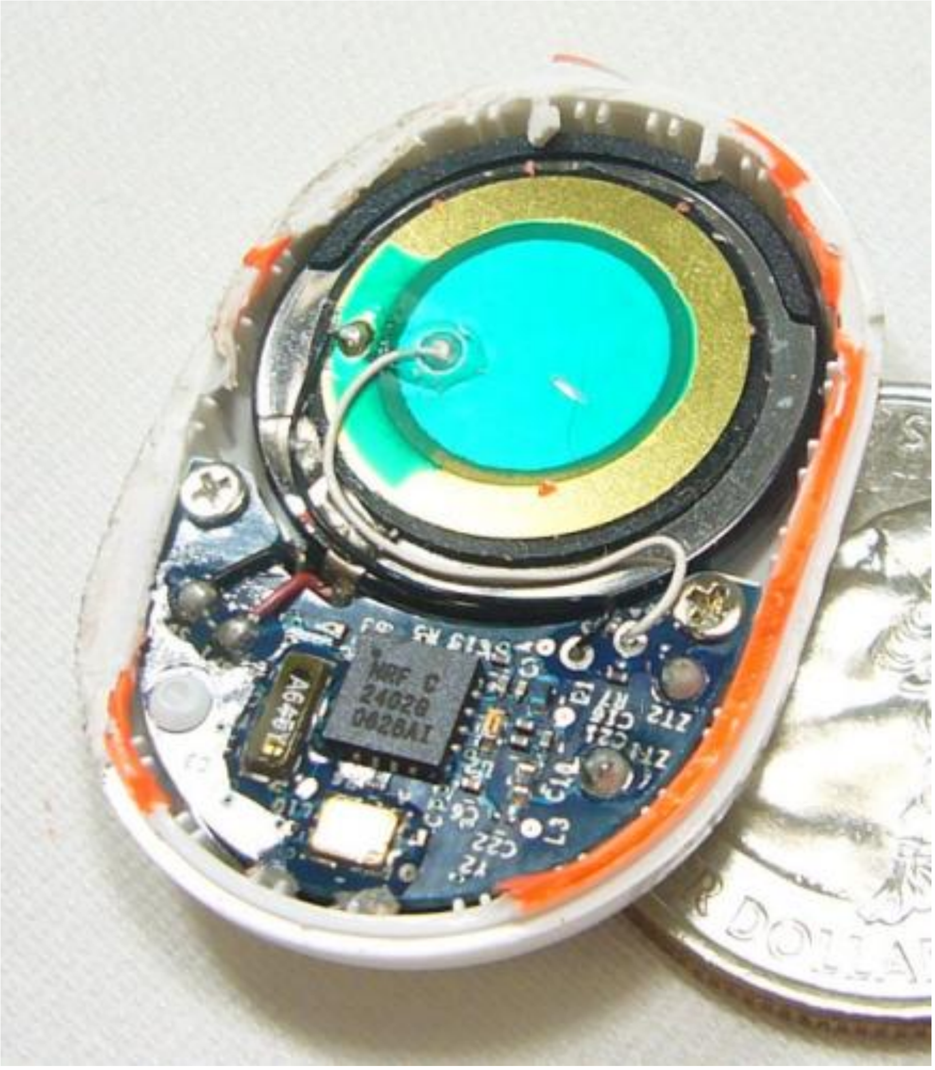
Good bye new friend.



Both receiver (left) and transmitter (right) are surprisingly small.



With a hacksaw and a chisel...



The insides revealed themselves! Immediately I was excited! That is the nRF2402 transmitter from Nordic VLSI which is just the lower-cost (transmit only) version of the transceiver (nRF2401A) that SparkFun Electronics has been using for years!

The A645Y block next to the nRF IC is what I believe to be a 32.768kHz oscillator to run the PIC 16F688 on the other side of the PCB. The small gold rectangle below the nRF IC is the 16MHz oscillator to run the nRF engine. And then a handful of caps, inductors, and resistors to run the RF engine and match to the antenna. You could probably match these passives to the example layout provided by Nordic. The Blue/Gold dot is the very cheap switch that activates when you take a step. It sits on top the 20mm Lithium coin cell battery.

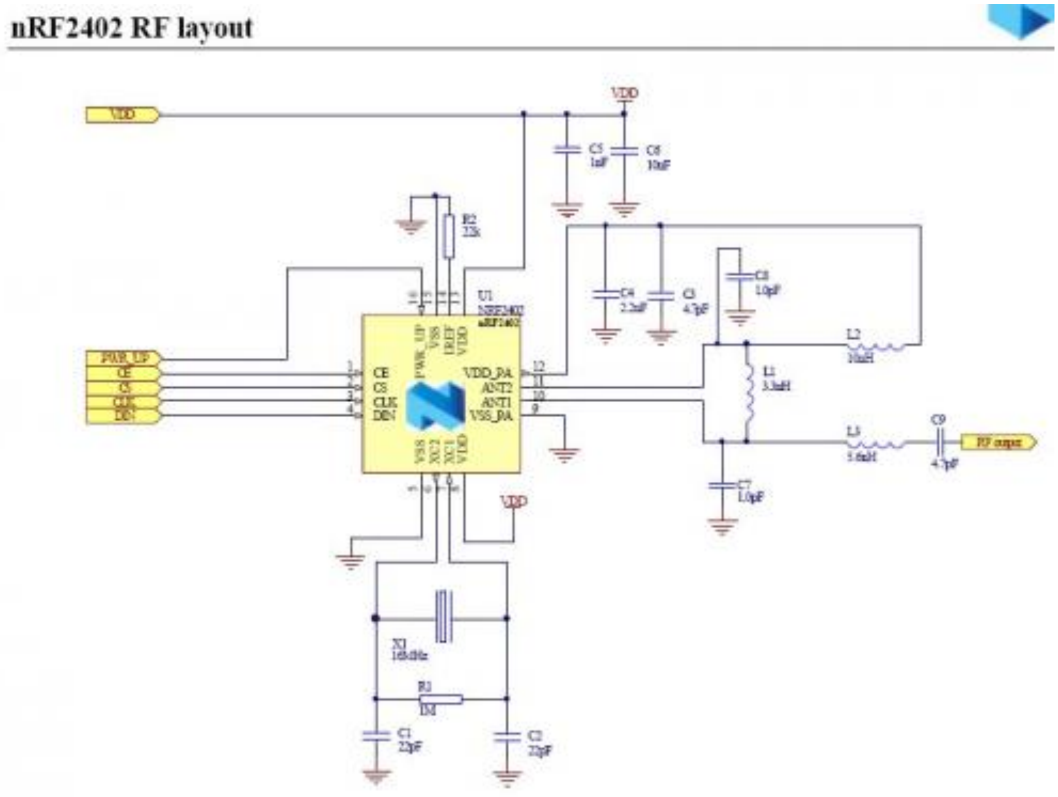
1-15-07 : A savvy SFE customer pointed out that the gold disc make be a bit more complex than originally thought: "I was just wondering whether the foot switch which you describe as, "..the Blue/Gold dot is the very cheap switch that activates..." is not in fact a piezoelectric disc? It looks strikingly familiar to the ones I've pulled from various toys that I couldn't help but look inside of when younger. They are commonly used as very cheap speakers in handheld games, however instead of putting volts into to get sound out, if you apply force, you get volts out. The only down side if it is one, is that they output a voltage almost proportional to the striking force they are hit with, ie soft blow = lowish voltage, swift hard blow = TENS of THOUSANDS of volts if not more. I'm sure the sparkfun community would be interested to see if this was the case, and perhaps you guys could have a go at investigating the effects of toasting one of these things if say your Nike thingo got damaged and a sharp blow was delivered to the piezo device :)"

Interesting idea. Could you run so hard as to blow your Nike+iPod? Probably not off this little pad, but it would be interesting to see if the module could detect *how hard* you were stepping as well as *how often* you were stepping.

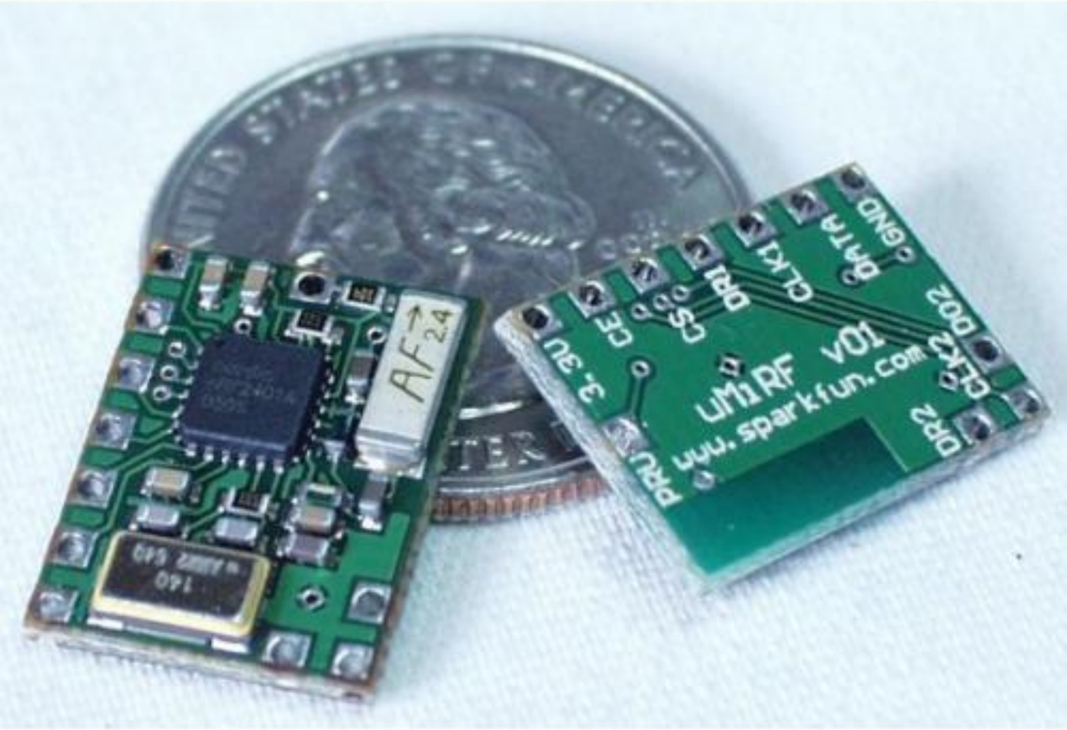
1-16-07 : Sure enough, straight from the horses mouth:

How does the sensor know how fast I am going?

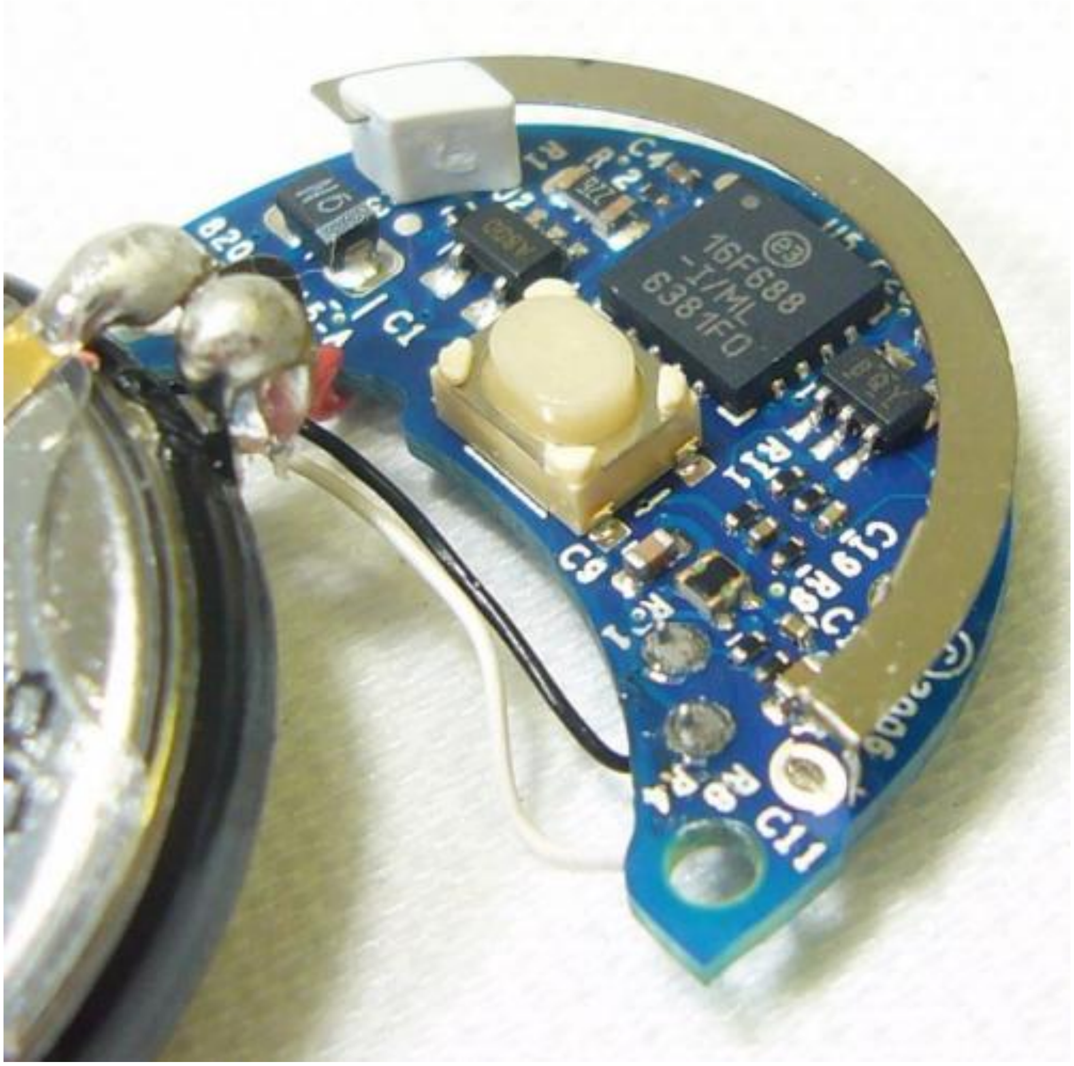
A sensitive piezoelectric accelerometer monitors your footstrike when you walk or run and determines the amount of time your foot spent on the ground. This contact time is directly related to your pace.



Example layout for the nRF2402.

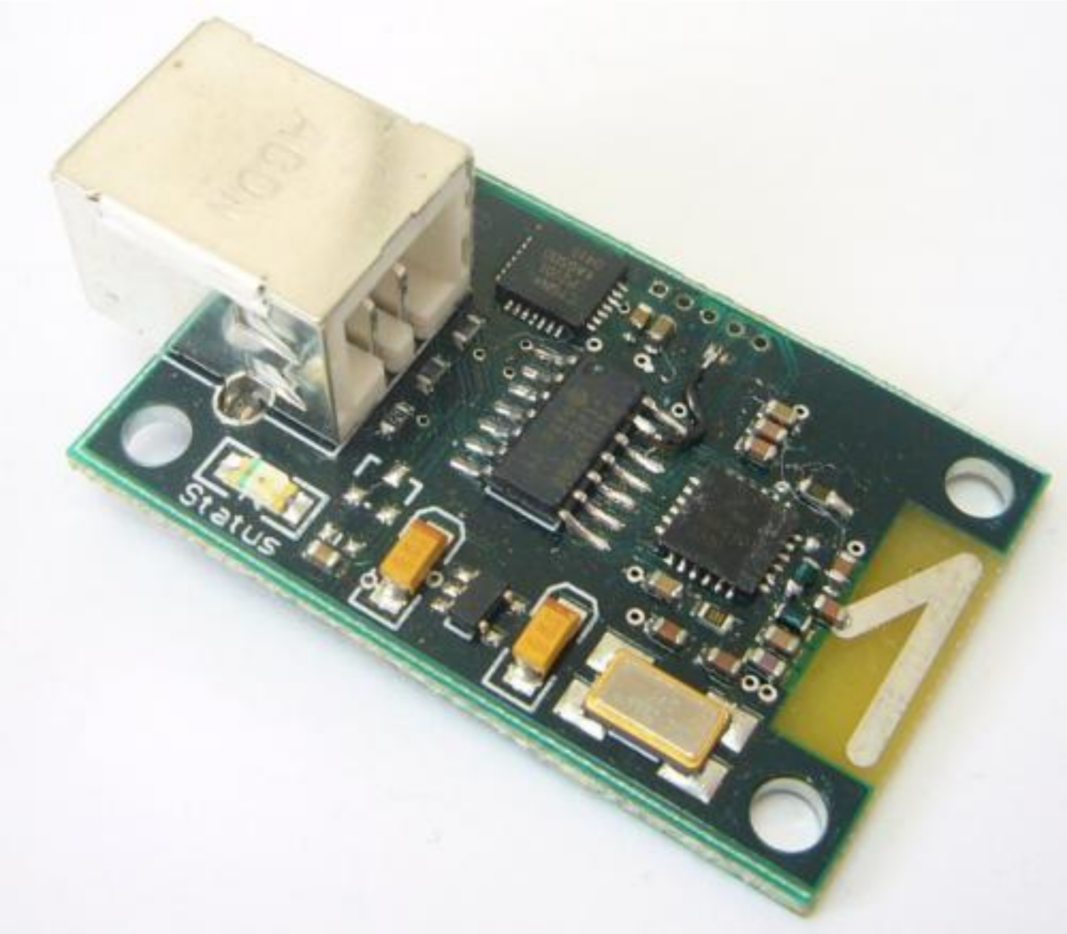


The uMiRF by SFE showing the big-brother nRF2401A. The nRF24xx series is a low-cost, very low-power RF device that operates in the 2.4GHz band. You can setup all sorts of fun protocols and data transmissions over short ranges (20-60ft).

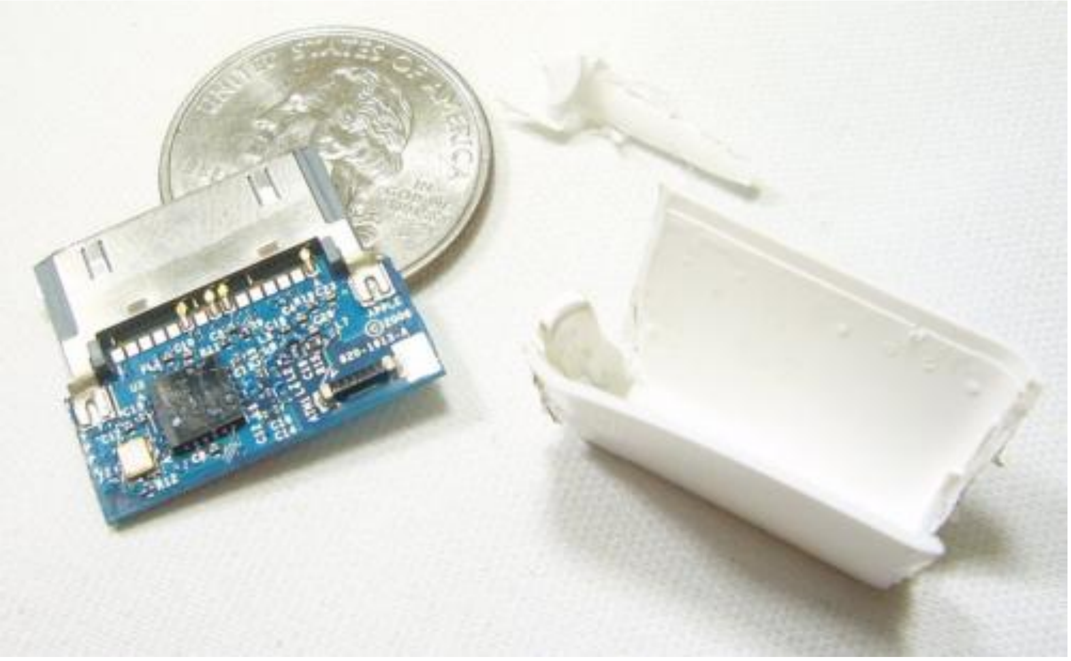


Are you kidding?! It's a PIC 16F688! Interesting choice for a big company like Nike/Apple. The 16F688 has some nice features and we've used that exact PIC to run an nRF IC, but Microchip (manufacturer of the PIC 16F688) has historically had poor pricing for larger volume customers. Perhaps Microchip is trying to break back into the volume market?

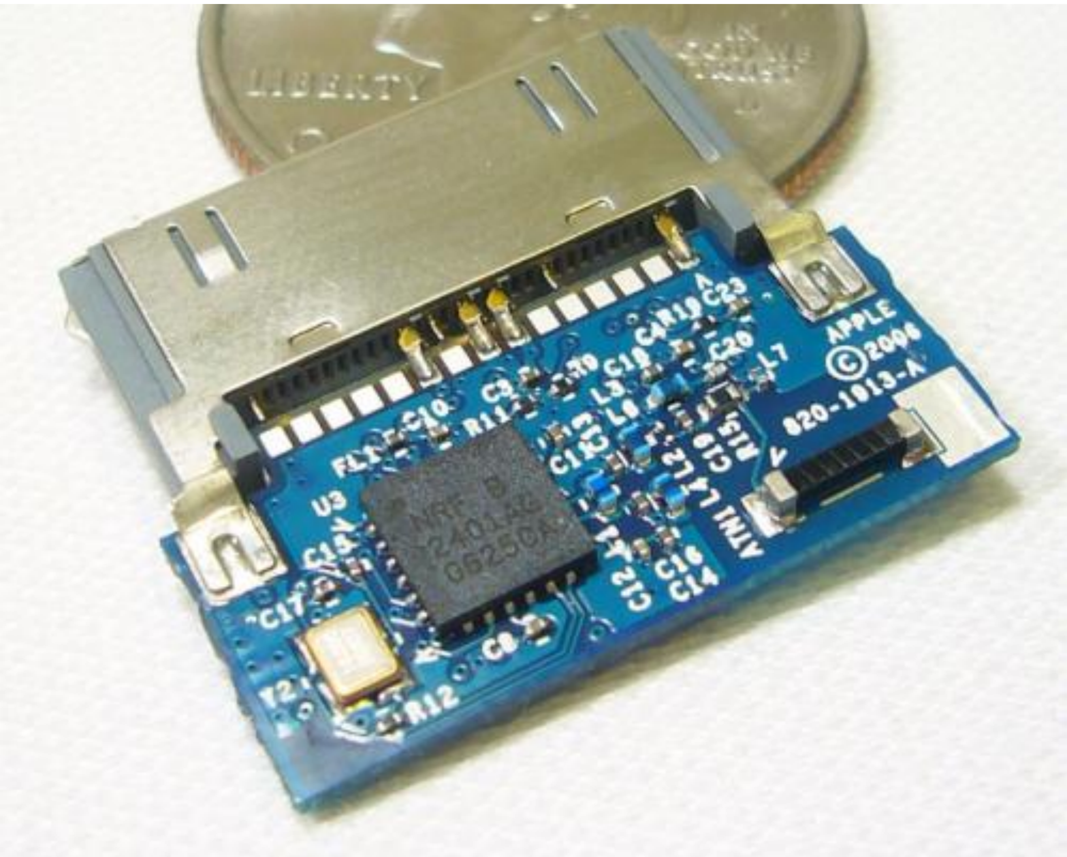
Here you see the Sleep/Wake button, voltage regulators?, and the large strip of metal that is a double-tapped monopole 2.4GHz antenna. Nicely done Nike/Apple! A strip of metal is cheap (reduce cost by $0.04) and the circuit has probably been tuned to match this antenna to get maximum range.



Here is the SparkFun's product using the same PIC 16F688 (larger SOIC package) and the nRF2401A IC with 16MHz xtal and PCB trace antenna. It's just scary how similar the technology is, and how important application of the technology is. This SFE device sold perhaps 50 units. The Nike+iPod has sold over a million.

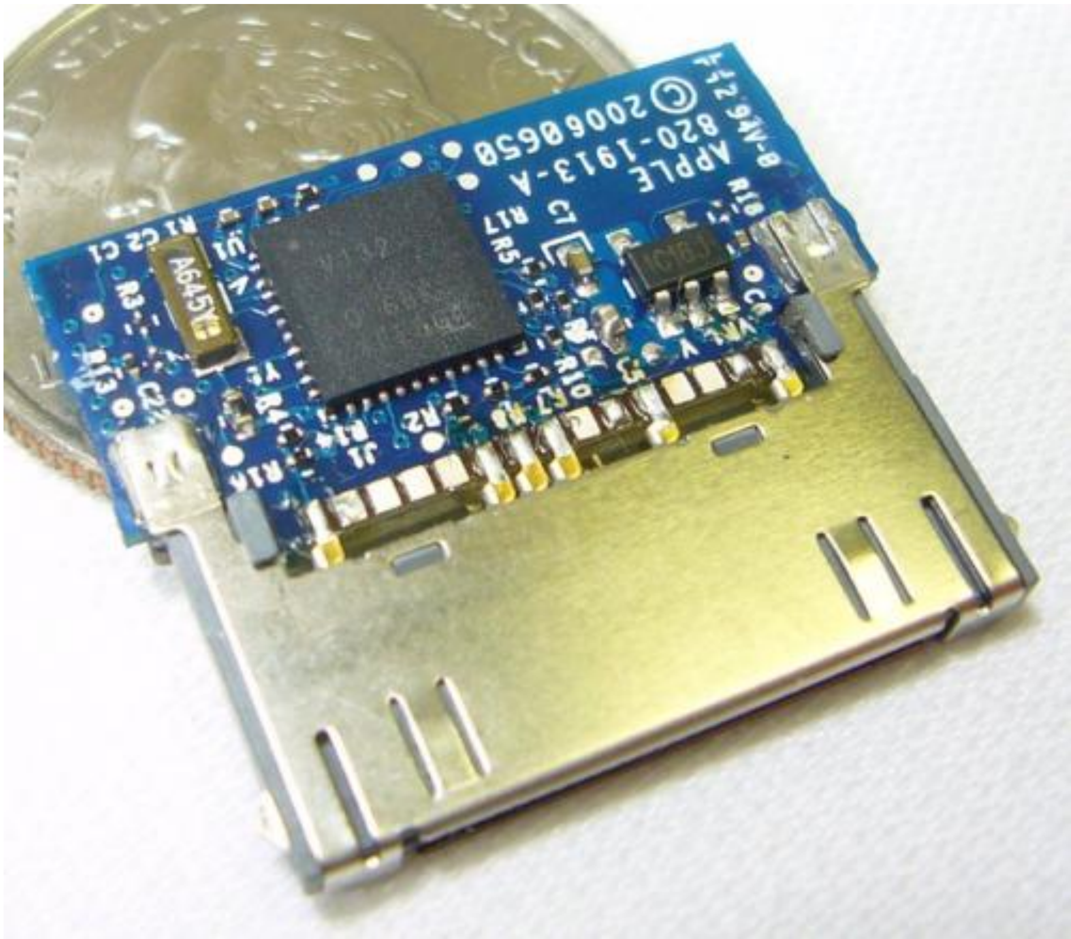


More chiseling and we've got the receiver opened up.



Nordic does not make a pure 'receiver'. Instead, Nike/Apple had to use the classic nRF2401A which is a *transceiver*. This means there is potential Apple programmed in some transmit features! It's possible that two of these units can be used to form a short-range link between iPods! I haven't a clue if Apple added this feature or not, but the hardware is there.

Same stuff here - the gold rectangle is the 16MHz oscillator for the nRF2401A, lots of Rs, Cs, and Ls (inductors), along with ATN1 which is a 50Ohm single feed 2.45GHz chip antenna. Probably more expensive than the strip of metal - but smaller.



Now this is what I would expect from Apple - what looks to be a custom ASIC to run the nRF engine and to pass serial strings to/from the iPod (if Apple can shave $0.10 from the BOM, they will). ASIC reads:

V132

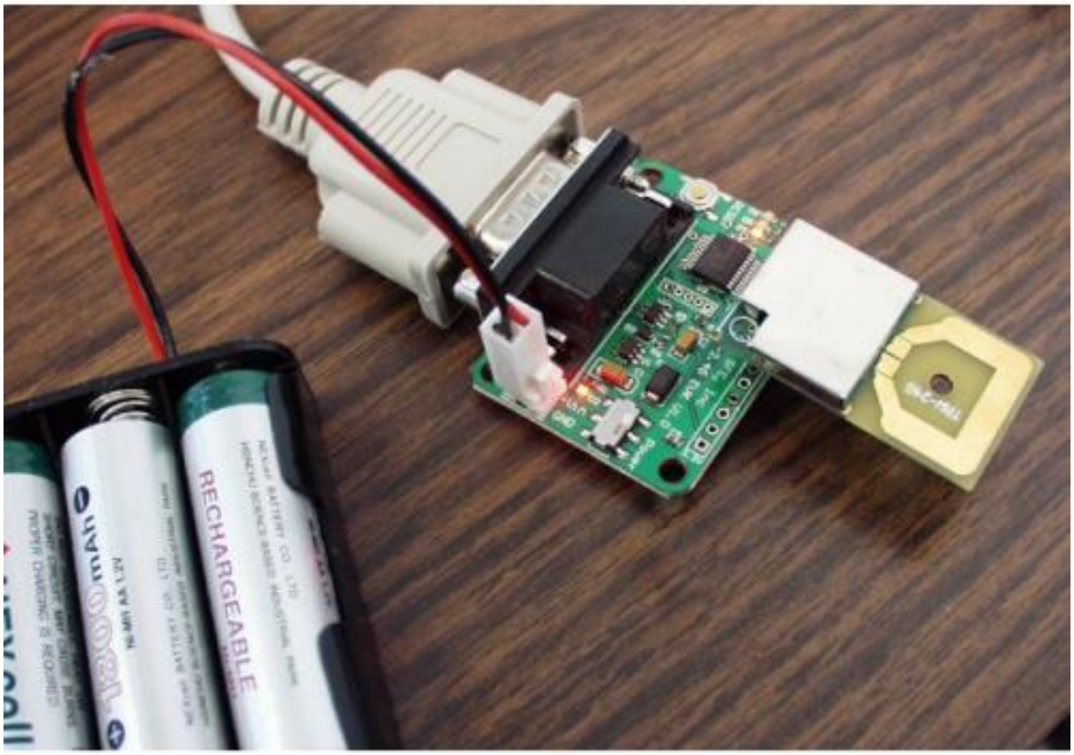
O 6BK

AEE6G4

Your guess is as good as mine. Looks like they used the same A645Y 32.768kHz oscillator to run this custom IC, plus a voltage regulator. I don't actually own an iPod so I can't hook it up to see what voltage this board runs at. Since the nRF2401A can run down to 1.9V, I would wager that the board is running at 2.8V.

The entire point of the foot pod was to run off a 3V battery for as long as possible. I think Nike/Apple did a good job of choosing some very low power technologies to squeeze every micro-amp out of the power supply. The PIC can wake from sleep, send out an ID string through the low-power nRF engine, and go back to sleep in a tiny fraction of a second.

Now for a discussion on what RF protocol the foot pod may be using. Originally, I wanted to use one of our nRF2401A devices and try to 'hear' a foot pod.



Here is a Transceiver Development Node featuring a PIC 16F88 (big brother to the 16F688) with serial interface and the RF-24G device which contains the nRF2401A. This setup would be completely able to hear any foot pod. The problem with the nRF24xx series is that it is so flexible that it's nearly impossible for us to guess what protocol Nike/Apple is using!

There are:

2 possible data rates (250k or 1mbit)

3 possible CRC configurations

8, 9, 10, all the way up to 40-bit address configurations

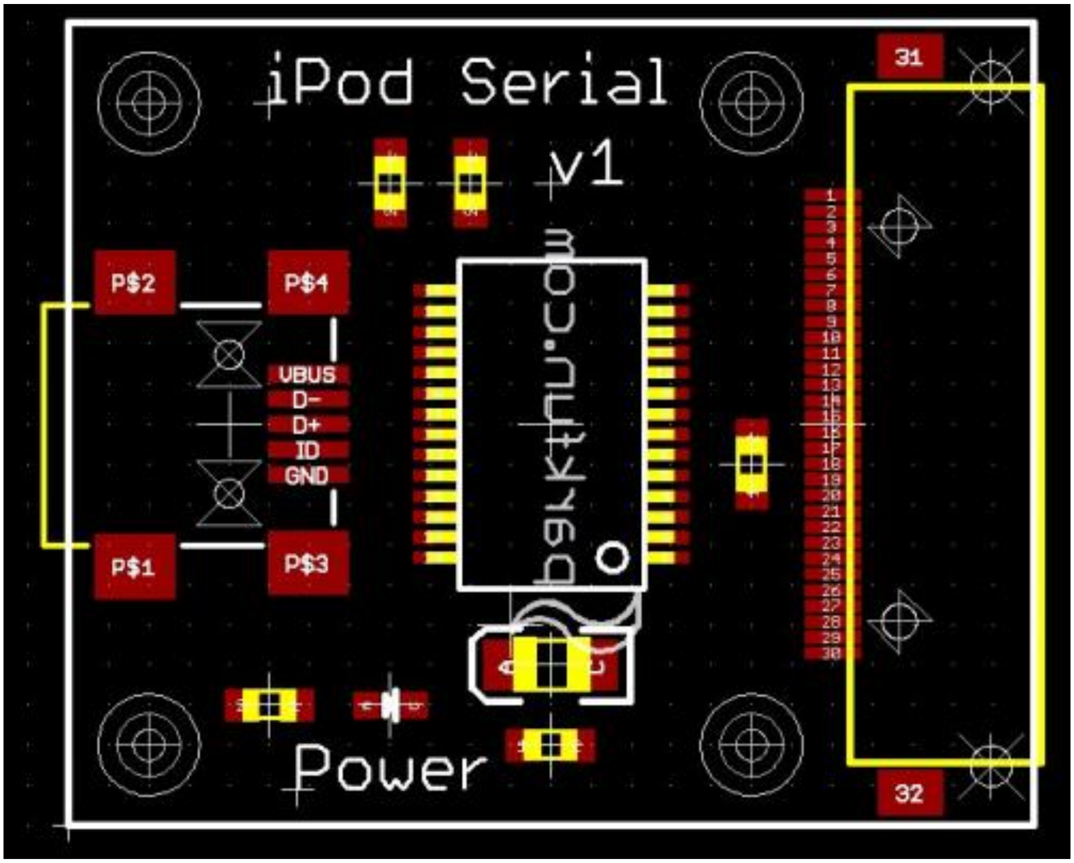
0 to 80 different channels the foot pods could be communicating on (chip can go up to channel 127 but FCC does not allow this)

Now, based on my own experience with the Nordic chipset, I can guess at a few things.

1. **16-bit Addresses** : Because of power consumption, you want to transmit the least amount of data humanly possible. This way the radio is on for the least amount of time. Therefore, 40-bit addresses are probably **not** used. 16-bits would be sufficient to be sure that two runners with Nike+iPods, running together, shouldn't experience cross-talk or data collisions (the odds are 1 in 65,535).
2. **1mbit data rate** : After using the nRF24xxs, the 250k bit rate works best for longer range applications, but the 1Mbit is faster (less time transmitting) and works great for <20ft (who's foot is more than 10ft away from their arm?).
3. **16-bit CRC** : CRC is almost mandatory for these ICs or else you get all sorts of trash on the link. 8-bit is ok, but I would say that 16-bit CRC is used just to make things as clean as possible. (This bends my first rule but an additional 8-bits of transmitted CRC data is not going to use a prohibitive amount of battery power.)
4. **One channel?** : Since the instruction manual gives steps on how to link to another foot pod sensor, we can gain some insight to how the iPod is scanning for sensors. There is no 'learn' or 'find me' button on the foot pod, so the receiver must know what channel and what address to listen initially. This would indicate that all food pods transmit on the same channel (or same small subset of channels) and on the same address.

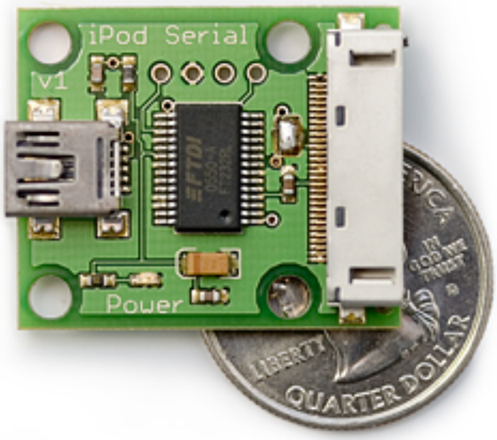
But that's really as far as I can postulate. To really find out, we're going to have to hot-air off the nRF2402 on the foot pod, solder on some wires for a scope, and try to get the PIC 16F688 to spill the beans (the PIC has to clock in the configuration word to the nRF before transmitting).

A much easier solution is to take the same approach as the University of Washington students - let the foot pod communicate with the receiver, and just talk to the receiver. The serial commands for the receiver are know, all I have to do is talk to it.



So here you go. A USB to serial adapter to talk directly to the Nike+iPod receiver. Now we just have to wait for the PCBs to come in...

I like this idea a lot. Where RFID requires you to physically get near a reader, this active foot pod can transmit over 10-20ft. You don't need to think about getting an RFID card out of your wallet, you just let your shoes do the talking.



It works! Sorry it took so long. The units are available here. We added a VCC/GND/TX/RX header so that you can eliminate the computer entirely and use an external microcontroller. This would allow you to build a small embedded device to listen for the correct foot pod ID and do something when the ID was heard. For example, a front door security system that unlocks when you, your kid, and your cat approaches the front door - and no one else. Perhaps a livestock monitoring system? The sky is the limit.

If someone gets their hands on an iPhone, please let us know (spark at sparkfun.com). We promise to send you the left over pieces.

January 13th 2007

SparkFun Electronics ® | Boulder, Colorado | Customer Service