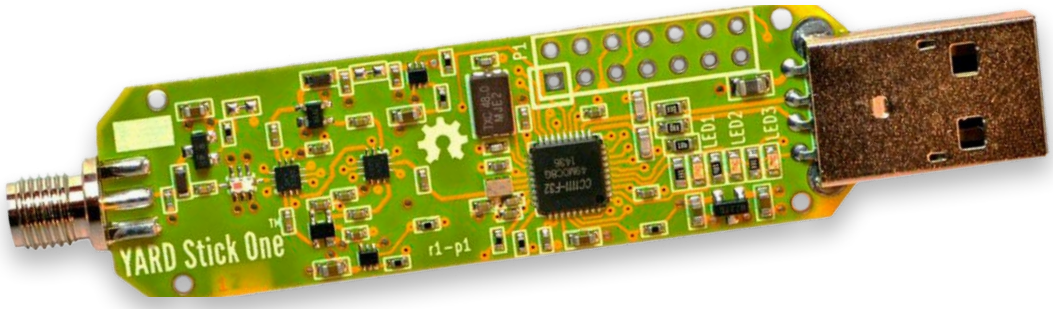
YARD Stick One

sub-1 GHz draadloos testtool



Wim Ton (Ierland)

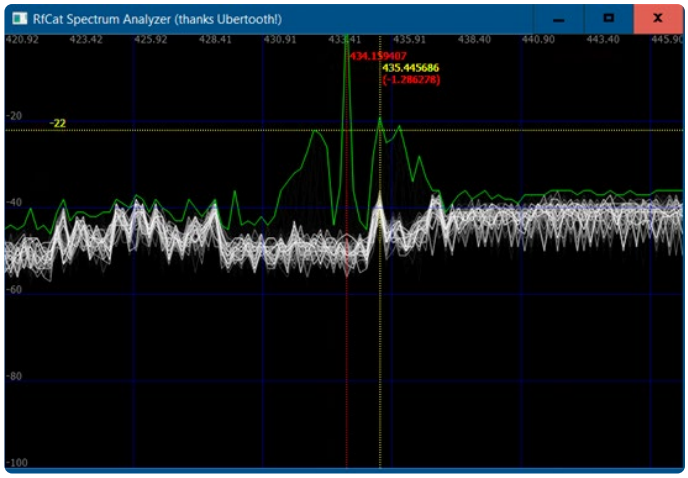
De YARD Stick One is een compacte 'hardware defined radio' die kan zenden en ontvangen in de UHF-band. Het is een soort breakout-board met een USB-interface om het gebruik op hosts zoals een PC of een Raspberry Pi mogelijk te maken. De YARD Stick One wordt geleverd met USB-software die is voorgeïnstalleerd in de 8051-core. De radio wordt bestuurd door een paar dozijn configuratieregisters te beschrijven, maar de Python-middleware kan veel van de details abstraheren.

Het belangrijkste voordeel van de YARD Stick One van Great Scott Gadgets is dat het een van de goedkopere apparaten is (vergeleken met de HackRF [1] of LimeSDR [2]) die ook kan zenden en min of meer 'plug and play' is, terwijl gewone, goedkope tools zoals de RTL SDR-dongles alleen kunnen ontvangen.
Aangezien alle low-level functies zijn geïmplementeerd in de vorm van een CC1111-chip [3], is het gebruik van de radio een kwestie van het correct schrijven van de configuratieregisters. De CC1111 is gericht op complexe Layer 2-protocollen, met functies zoals syncwords, framing, interleave en scrambling. Aangezien de CC1111 is ontworpen als een SoC voor commerciële RF-toepassingen, is het gebruik van de YARD Stick One voor signaalanalyse zeer beperkt. Tenzij het te testen systeem een vergelijkbare SoC gebruikt, is het minder frustrerend en goedkoper om een SDR te gebruiken.
De YARD Stick One wordt alleen ondersteund door *rfcat*, op Python gebaseerde middleware die de meest gebruikte opties abstraheert in een soort beschrijvende methode. Voor fijnafregeling biedt *rfcat* ook directe registertoegang.
Bij levering is het apparaat een print zonder behuizing die met de nodige zorg moet worden behandeld. Behuizingen van derden zijn beschikbaar.
De term 'sub-1 GHz' is een beetje (te) breed; de YARD Stick One is beperkt door zijn TI CC1111-radio, die de lagere UHF ISM-banden dekt: 300...928 MHz. Met name de 13,56 MHz band, die wordt gebruikt voor RFID, wordt niet bestreken.
De YARD Stick One werkt iets stabieler onder Linux dan onder Windows 10. Windows herkent het apparaat vaak helemaal niet, maar onder Linux lukt het meestal met herhaaldelijk loskoppelen en insteken van het apparaat.

Installatie van de software

Voor het gebruik van de YARD Stick One is een goed begrip van OSI-lagen 1 en 2 vereist. Enige kennis van Python en bekendheid met het beoogde besturingssysteem is ook nuttig om installatieproblemen op te lossen. De software die wordt aanbevolen in de Elektor-store [4] werd geïnstalleerd onder Windows 10, Kali en Ubuntu 18.
De installatie van *rfcat* [5] onder Linux met Python 3.10 werkte goed. Het enige verschil met de documentatie was dat *rfcat* gestart moet worden met

```
./rfcat
```



Figuur 1. Spectrumweergave in rfcat.

Als je een '`Error in resetup()`' krijgt, koppel dan het apparaat los en steek het opnieuw in.
Windows 10: installeer Python niet via Microsoft Store, omdat dit de bestandsrechten in de war schopt; installeer handmatig voor alle gebruikers. Daarnaast moet je invoeren:

```
pip install Cython
```

Installeer in ieder geval met admin-privileges (zie waar de Linux-instructies `sudo` vereisen). En zorg ervoor dat je een VC > 14 hebt geïnstalleerd.
Vereiste aanpassing als je een foutmelding krijgt over 'collections not callable': voeg `.abc` toe in *C:\Program Files\Python310\Lib\site-packages\pyreadline\py3k_compat.py* op regel 8:

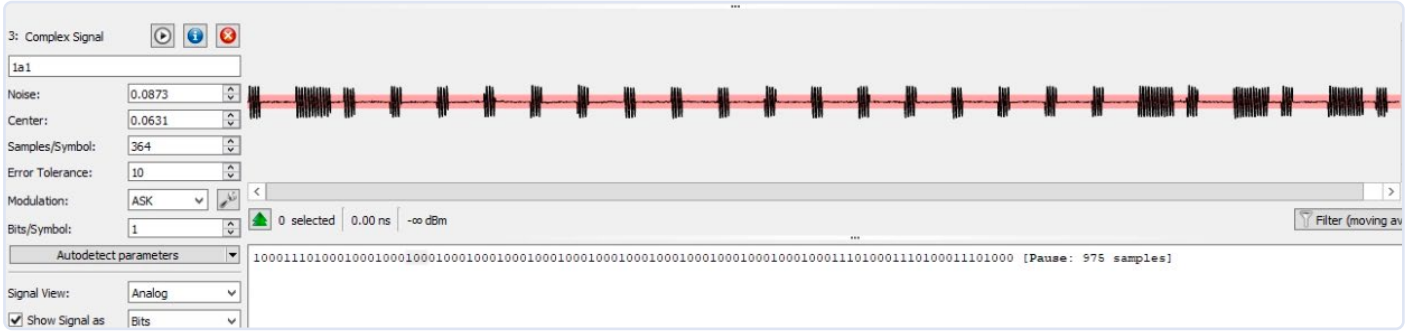
```
return isinstance(x, collections.abc.Callable)
```

Er wordt gezegd dat *pyreadline* alleen nodig is voor Windows.
Installeer de sriver *libusb-win32*. De eenvoudigste manier is waarschijnlijk met *Zadig* [6], dat meestal wordt geleverd met *SDR#*. Als het apparaat afwezig is, krijg je de uitzondering 'No Dongle Found' van *rfcat*. Bij een 'ChipconUsbTimeoutException' moet de tool loskoppelen en opnieuw insteken. Al met al is de installatie en het gebruik onder Windows 10 een beetje lastiger dan onder Linux. Je moet `setmodeIDLE()` aanroepen aan het einde van het script, anders zal er een 'device not found' fout optreden bij de volgende maal opstarten.

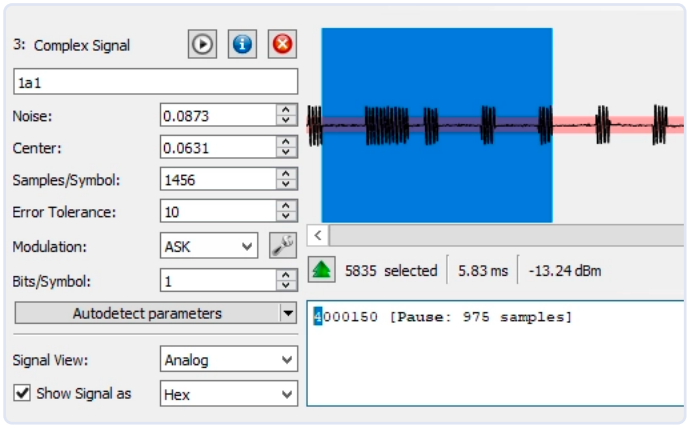
De controller die in de CC1111 wordt gebruikt is een MCS51-variant en heeft SDCC (Small Device C Compiler) [7] versie 3.5 of lager nodig. Het vereist enig handwerk tijdens de installatie, aangezien de huidige versie 4.x is. Veel gebruikers zullen echter gewoon de *rfcat*-firmware gebruiken.

Gebruik van de YARD Stick One

De CC1111-radio doet al het low-level werk, het toevoegen en verwijderen van pre- en postambles, syncwoorden, CRC, plus modulatie en demodulatie. De radio moet volledig geconfigureerd worden voor gebruik, aangezien de resetconfiguratie nutteloos is. Het schrijven van een klein Python-programma zoals beschreven in [8] bespaart een hoop typewerk en fouten.
rfcat biedt ook spectrumweergave. Het een 'analyzer' noemen is wat overdreven – de meeste van de simpeler apparaten hebben een beperkte bandbreedte en dynamisch bereik, in tegenstelling tot de zware jongens zoals de HP141 of HP181 die 1 GHz bandbreedte kunnen weergeven met een dynamisch bereik van 80 dB.
Om de YARD Stick One als ontvanger te gebruiken, moeten de Layer 1- en Layer 2-eigenschappen correct worden geconfigureerd, anders zal de radio het package negeren. Om een onbekend signaal te analyseren is een extra SDR nodig; de goedkoopste hardware hiervoor wordt gevormd door de RTL-dongles. Naast het gebruik van GNU Radio en Audacity zoals getoond in [9], biedt de Universal Radio Hacker [10] een meer geïntegreerde workflow voor signaalanalyse en -replay. Als alternatief kan de instelling van de radiochip worden afgeleid uit de hardware-interface als het type chip bekend is, zoals getoond in [11].
Het gebruik van de YARD Stick One als generieke ontvanger is nogal onhandig: bij te ruime instellingen wordt veel ruis ontvangen; bij te krappe instellingen wordt alles weggefilterd. Het zou kunnen werken met een variabele verzwakker aan de ingang, maar die had ik niet bij de hand.
Bij de configuratie van de vele registers van de CC1111 komt het hulpprogramma SmartRF Studio van TI [12] van pas. De berekende waarden kunnen naar de YARD Stick One worden geschreven met de juiste `setXxx(value)`-functie.
De firmware zoals geleverd bij de YARD Stick One in de Elektor Store fungeert als brug tussen de CC1111-registers en de USB-interface.



Figuur 2. Symbool-aanzicht.



Figuur 3. Gegevens-aanzicht.

Na een Python-exception moet de YARD Stick One worden losgekoppeld en opnieuw worden ingestoken, anders vindt *rflib* hem niet meer. Het volgende voorbeeld toont een PWM-signaal met ASK-modulatie, wat heel gebruikelijk is voor eenvoudige afstandsbedieningen. De schermafbeeldingen zijn van URH.
Elke databit bestaat uit vier symbolen, een 0 wordt verzonden als 1000 en een 1 wordt verzonden als 1110, dus dit moet naar de YARD Stick One worden verzonden als 8e888888888888888e8e8e8e8e8. Eén symbool duurt 0,484 ms, dus de baudrate moet worden ingesteld op 2744.

Documentatie

De documentatie [4] waarnaar de Elektor Store verwijst, is erg summier. Het forum waar Great Scott Gadgets naar verwijst, is van beperkt nut. De *rfcat* git-repository geeft veel informatie over het bouwen en downloaden van de YARD Stick One-firmware. Er zijn enkele tutorials op het internet, zie bijvoorbeeld [13]. Houd je aan de lokale regels voor de ISM-band.

Conclusie

De YARD Stick One is niet goedkoop voor wat hij te bieden heeft, en hij heeft een vrij steile leercurve. De software is niet perfect en de documentatie is aan de lichte kant. Alleen voor analyse is een eenvoudige SDR-ontvanger een veel betere keuze. Voor zenden heb je al een generieke SDR-ontvanger voor € 150 meer (bijvoorbeeld HackRF One of Adalm Pluto).
De YARD Stick One kan nuttig zijn als je je concentreert op de specifieke protocollen die door deze familie van radio-SoC's ondersteund worden. (Zie IM-Me [14] zoals genoemd op de Elektor-site.) Voor specifieke toepassingen zou je een CC111x breakout board [15] uit China kunnen overwegen, aangesloten op een Arduino, die de lastige USB-communicatie vermijdt.

230388-03

Vragen of opmerkingen?

Hebt u technische vragen of opmerkingen naar aanleiding van dit artikel? Stuur een e-mail naar de redactie van Elektor via redactie@elektor.com.

Gerelateerde producten

- **Great Scott Gadgets YARD Stick One – Sub-1 GHz Wireless Test Tool**
  www.elektor.nl/20088
- **Great Scott Gadgets HackRF One Software Defined Radio (1 MHz to 6 GHz)**
  www.elektor.nl/18306
- **Great Scott Gadgets GreatFET One Universal USB**
  www.elektor.nl/19114
- **Elektor Raspberry Pi RTL-SDR Bundle (pre-order)**
  www.elektor.nl/19518

WEBLINKS

[1] Denis Meyer, "HackRF One SDR transceiver: van 1 MHz tot 6 GHz":
http://www.elektormagazine.nl/news/hackrf-one-sdr-transceiver-van-1-mhz-tot-6-ghz
[2] Jan Buiting, "Digitale TV-zender met een Raspberry Pi Zero en LimeSDR Mini":
http://www.elektormagazine.nl/news/digitale-tv-zender-met-een-raspberry-pi-zero-en-limesdr-mini
[3] CC1110Fx / CC1111Fx datasheet: https://ti.com/lit/gpn/cc1110-cc1111
[4] YARD Stick software en documentatie: https://github.com/greatscottgadgets/yardstick
[5] RfCat GitHub: https://github.com/atlas0fd00m/rfcat
[6] Zadig: https://zadig.akeo.ie/
[7] SDCC: http://sdcc.sourceforge.net/
[8] YARD Stick One opmerkingen: https://bit.ly/3ql6mjo
[9] Hacking Everything with RF and Software-Defined Radio - Part 1: https://bit.ly/3qpIGul
[10] Universal Radio Hacker: https://github.com/jopohl/urh
[11] Radio Communication Analysis using RfCat: https://bit.ly/42kxvAj
[12] SmartRF Studio van Texas Instruments: https://ti.com/tool/smartrftm-studio
[13] Hacking Everything with RF and Software-Defined Radio - Part 2: https://bit.ly/43ITm5D
[14] Een zak-spectrumanalyzer van $16: https://ossmann.blogspot.com/2010/03/16-pocket-spectrum-analyzer.html
[15] CC111x breakout board: https://www.aliexpress.com/item/32963409008.html