Spread spectrum techniques in disposable drones for anti drone evasion



David Meléndez Cano

@TaiksonTexas

I+D & Embedded Software Engineer

Drone and Robot Builder
(Atropos & Interceptor Drones + Texas Ranger ROV)

Author of the book
"Hacking con Drones"



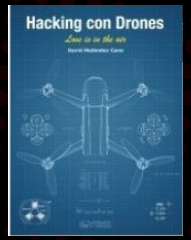
Gabriela García

@constrainterror

Secure Software Developer

Hacker and hacking communities co-organizer

Coding & Cybersecurity instructor & mentor



black hat

DEFCON

Campus Party™

NUIT DU HACK

HONG KONG OPEN SOURCE CONFERENCE

/Rooted

{codemotion}

HACKMADRID %27

%27

JS Day CANARIAS

Context: a World in War



Drones as War Elements





Drones as War Elements

- Directed weapons
- Unmanned
- Elements for symmetric warfare
- Means of strategy and tactics for real-time covert operations

Drones as War Elements: Directed Weapons



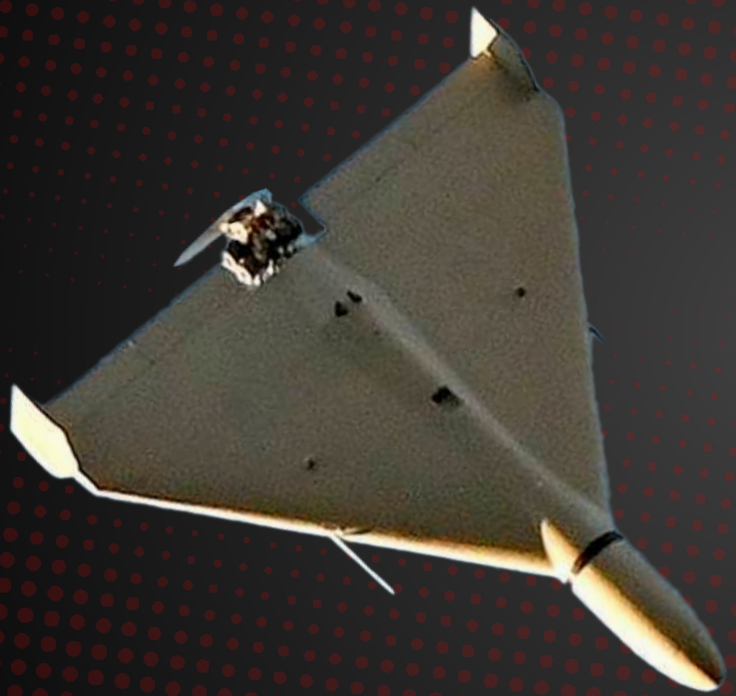
➢ **High attack precision**: lower collateral damage and civilian casualties.

➢ **Reduction of human risk** by being operated remotely.

➢ **Extended operations** without having to worry about fatigue.

➢ **Versatility**: equipped with a variety of weapons, from missiles to bombs.

Drones as War Elements: Symmetrical Warfare



➢ **Lower cost effectiveness** compared to traditional manned aircraft.

➢ **Cost reduction in drone production** (cardboard drones, wooden drones, 3D printing, cheap chipsets, etc.)

Drones as War Elements: Strategy



➢ **Means of strategy and tactics** for real-time covert operations.

➢ **Surveillance capability and data collection** for intelligence purposes.

Use of drones for SIGINT (Signals Intelligence)



➢ **Collection of information**, interception, and analysis of enemy communications and electronic signals.

➢ **Extended reach** to hard-to-access areas.

➢ **Prolonged operations** continuously collecting data.

➢ **Real-time transmission of information** for analysis, enabling quick response to emerging threats.

➢ **Covert operations** from high altitudes or in discreet flight patterns.

Anti-drone measures



➤ **Thermal and standard cameras** for shape detection.

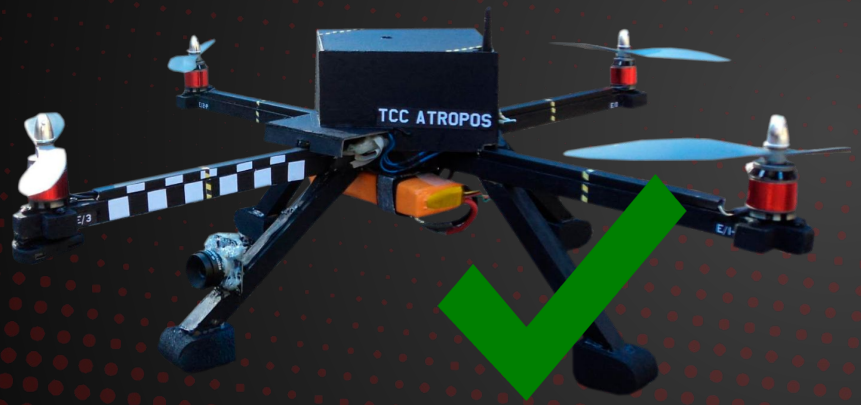
➤ **Detection of heat** emitted by engines and electronics.

➤ **Characterization** of drone noise.

➤ **Radio frequency and waveform detection**.

➤ **Radio signature**.

Counter-Countermeasures



- **Frequency hopping**
- Utilization of **unexpected frequencies** by the jammer
- **Robust protocols**
- **Physical attacks**

EVOLUTION OF ‘ATROPOS’ AS A WAR WEAPON



ATROPOS

- WiFi Router
- PIC16F876 for PWM
- Wii Nunchuck and
- Motion + as onboard IMU
- HTML5 telemetry by router
- Webserver
- WiFi
- WPS Attacks with bully



EVOLUTION OF ATROPOS: STAGE 1

➤ Avoiding deauthentication attacks with **Beacon Frames**

➤ Using beacon frames to **deceive adversary SIGINT** by creating fictitious drones



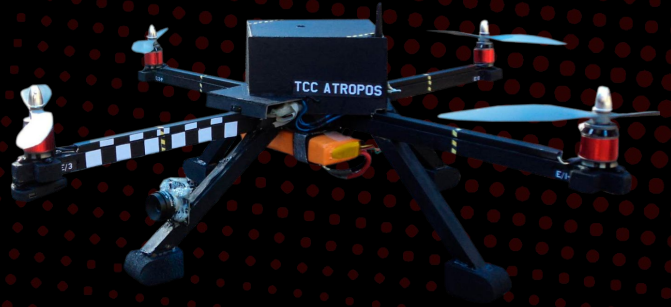
EVOLUTION OF ATROPOS: STAGE 2

➤ Testing a **new concept of mini-drone (INTERCEPTOR)** with the ATROPOS model.



➤ Adding autonomous hacking capabilities **using the drone's own hardware**.

➤ Incorporating a **control side-channel using an FM transmitter**.



2012-2014



USB



WIFI STA-AP



2014-2017



USB



WIFI BEACONS

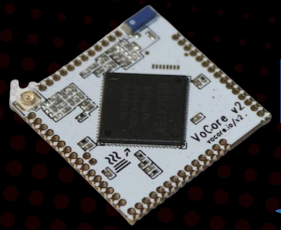




2018



USB



WIFI BEACONS

WIFI BEACONS

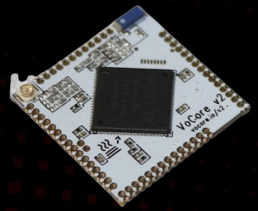




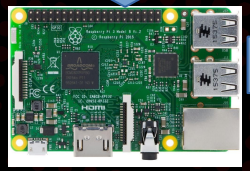
2020



USB



LAN



WIFI BEACONS

WIFI BEACONS



I2C



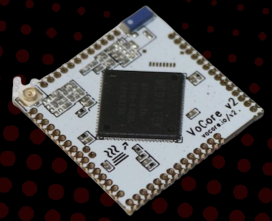
FM RDS PAYLOAD

Associated Experiments: Interceptor



USB





WIFI BEACONS

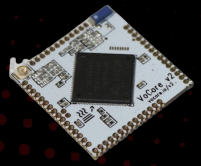
WIFI BEACONS



Associated Experiments: Interceptor



USB



LAN





I2C

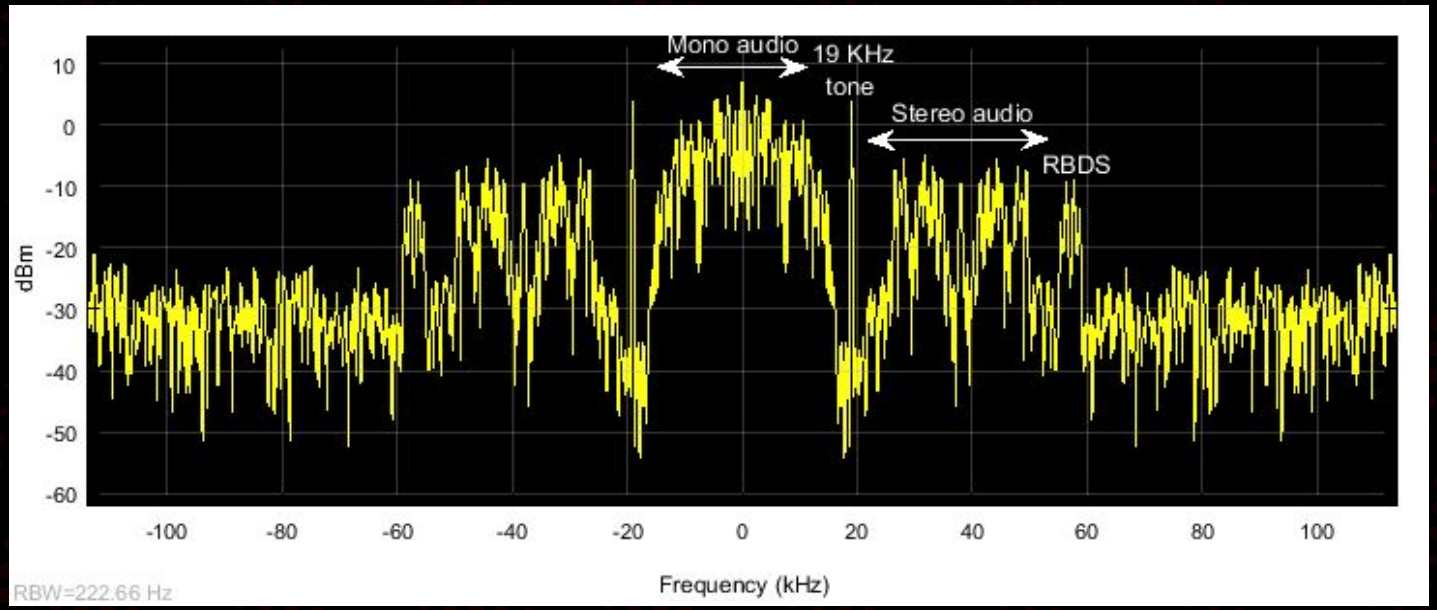
WIFI BEACONS

WIFI BEACONS

FM RDS PAYLOAD



RDS FM


Mono audio
19 KHz
tone
Stereo audio
RBDS
10
0
-10
-20
-30
-40
-50
-60
dBm
-100
-80
-60
-40
-20
0
20
40
60
80
100
Frequency (kHz)
RBW=222.66 Hz

EVOLUTION OF ATROPOS: STAGE 3

WAR WEAPON



EVOLUCIÓN DEL ATROPOS: STAGE 3

➢ **Step 1**: Controlling the drone through arbitrary frequency generation



EVOLUCIÓN DEL ATROPOS: STAGE 3

➢ **Step 2:** Signal reception using SDR (Software-Defined Radio) within the drone.



EVOLUCIÓN DEL ATROPOS: STAGE 3

➤ **Step 3:** Application of spread spectrum using frequency hopping method.

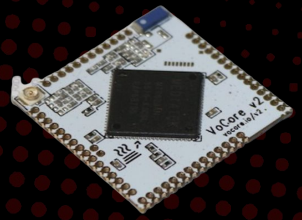




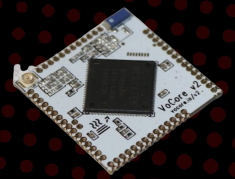


USB

LAN



I2S 2ASK MODULATION





SPREAD SPECTRUM

Spread spectrum is a **modulation technique that distributes the signal over a much wider frequency band** than what is required by the original information.

The use of spread spectrum **improves resistance to noise and interference**, as a signal spread over a wider spectrum can better tolerate noise at a specific frequency.

SPREAD SPECTRUM

- FHSS

  Frequency Hopping Spread Spectrum

- DSSS

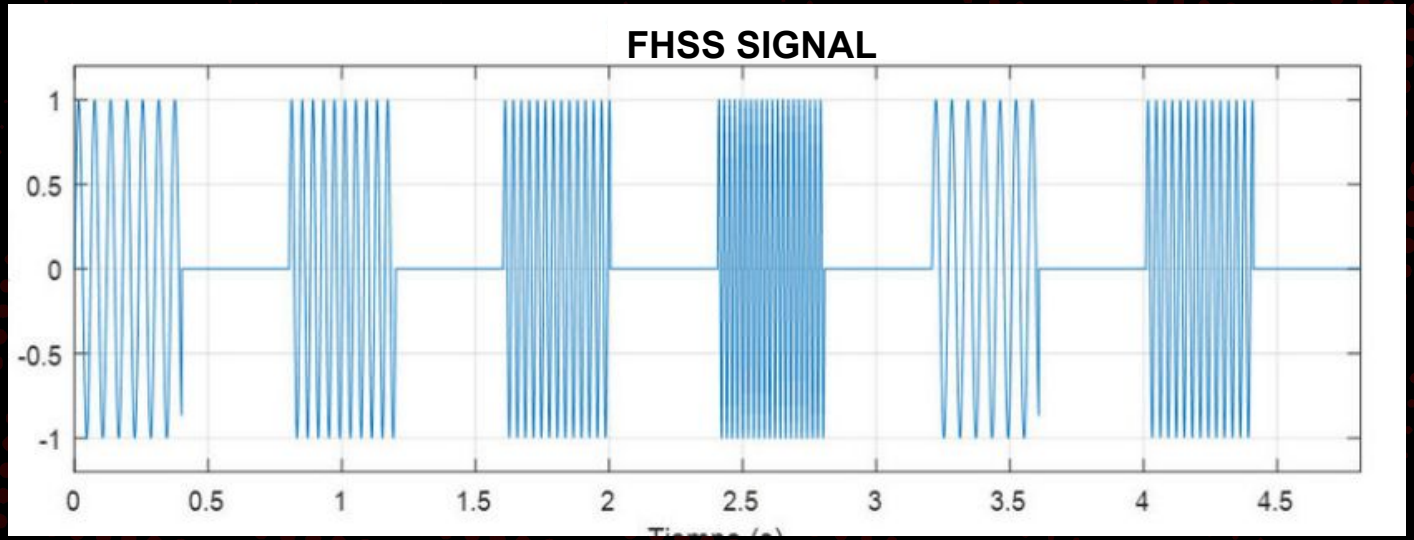
  Direct Sequence Spread Spectrum





FREQUENCY HOPPING SPREAD SPECTRUM (FHSS)

In FHSS, the data signal is transmitted over different frequencies in a predetermined pattern that only the receiver knows and can track.



¿Would it be possible with an MT7628?

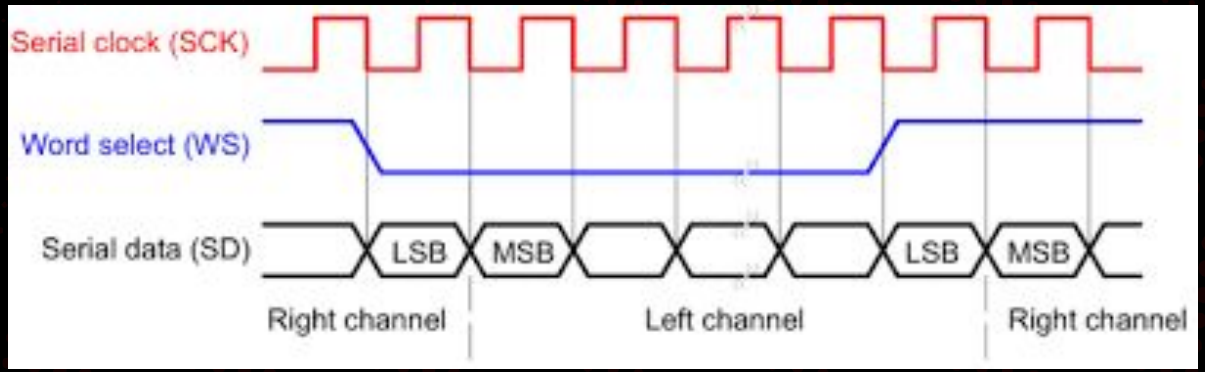
HOLD MY



BEER

I2S BUS

- Audio digital interface
- ***IT IS NOT I2C BUS***
- CLOCK PIN
- PIN DATA TX
- PIN DATA RX

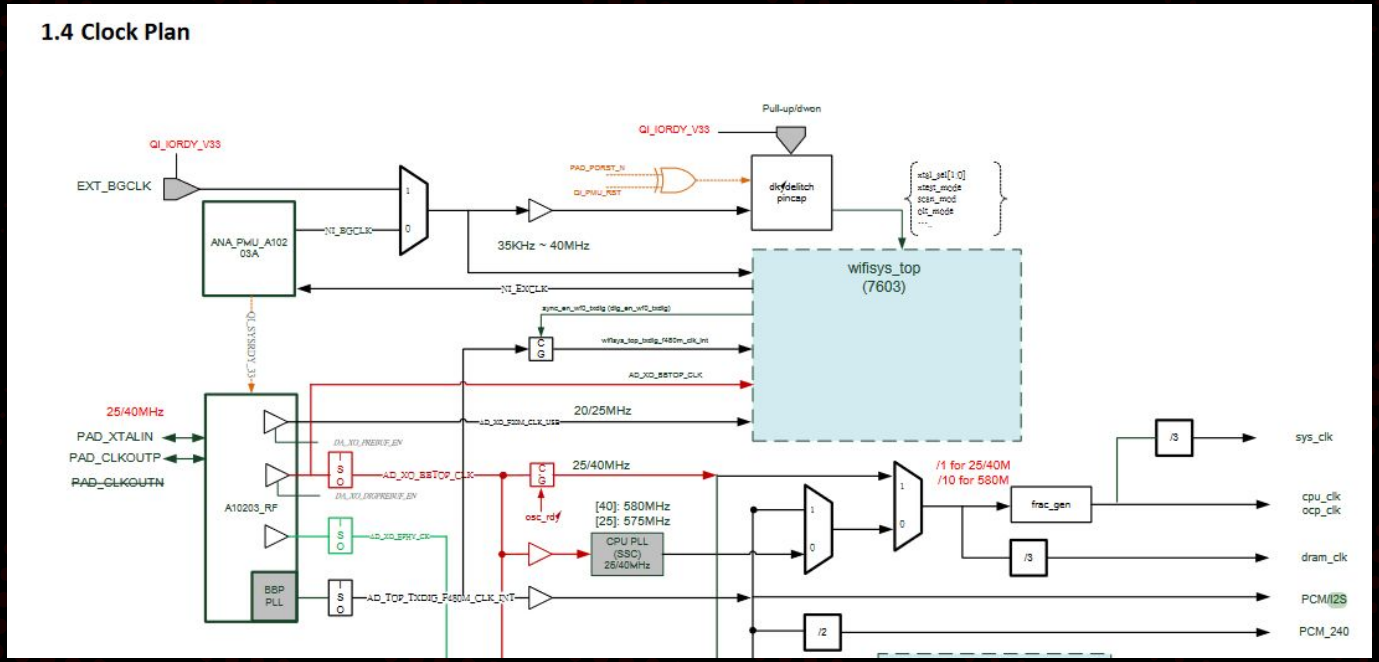


I2S Schema in Mediatek MT7628

I2S				
16	I2S_SDI	O	4 mA	I2S data input
17	I2S_SDO	I/O, IPD	4 mA	I2S data output
18	I2S_WS	O	4 mA	I2S word select
19	I2S_CLK	I/O	4 mA	I2S clock

1000.0A00	-	1000.0AFF	256 Bytes	I2S

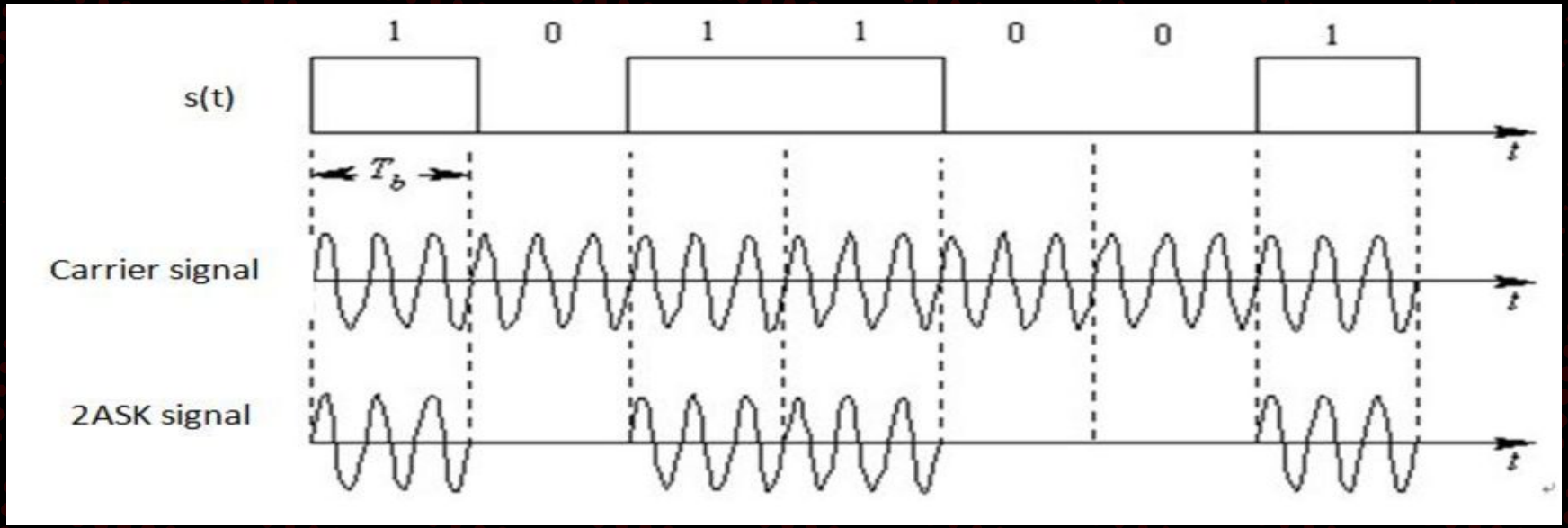
1.4 Clock Plan



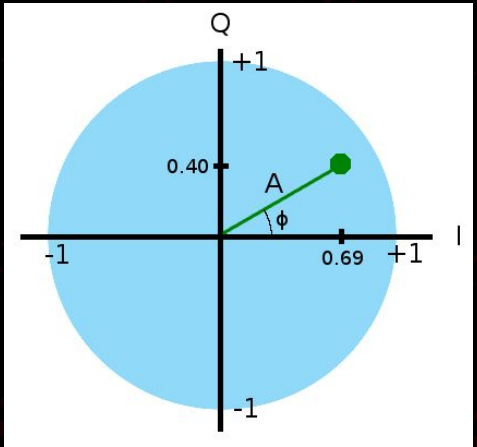
Module name: I2S Base address: (+10000A00h)

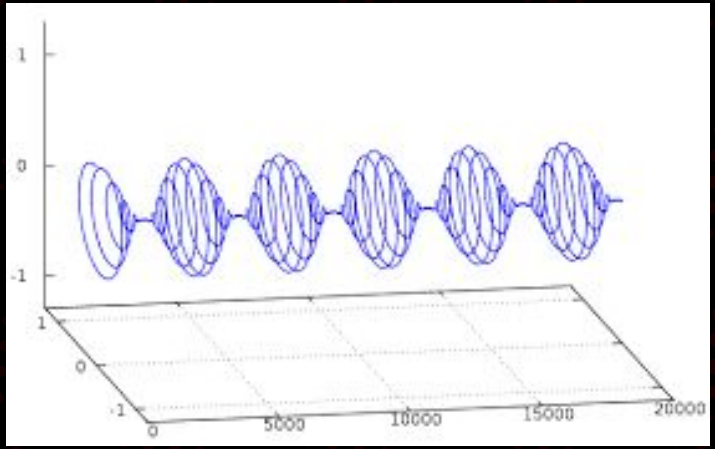
Address	Name	Width	Register Function
10000A00	I2S_CFG	32	**I2S Configuration** I2S Tx/Rx Configuration Register
10000A04	INT_STATUS	32	**Interrupt Status** I2S Interrupt Status
10000A08	INT_EN	32	**Interrupt Enable** I2S Interrupt Enable Control Register
10000A0C	FF_STATUS	32	**FIFO Status** I2S Tx/Rx FIFO Status
10000A10	TX_FIFO_WREG	32	**Transmit FIFO Write to Register** Tx Write Data Buffer
10000A14	RX_FIFO_RREG	32	**Receive FIFO Read Register** DRAM PAD CONTROL 3
10000A18	I2S_CFG1	32	**I2S Configuration 1** I2S Loopback Test Control Register
10000A20	DIVCOMP_CFG	32	**Integer Part of the Dividor Register 1** Integer Part of the Dividor Register
10000A28	DIVINT_CFG	32	**Integer Part of the Dividor Register 2** Integer Part of the Dividor Register

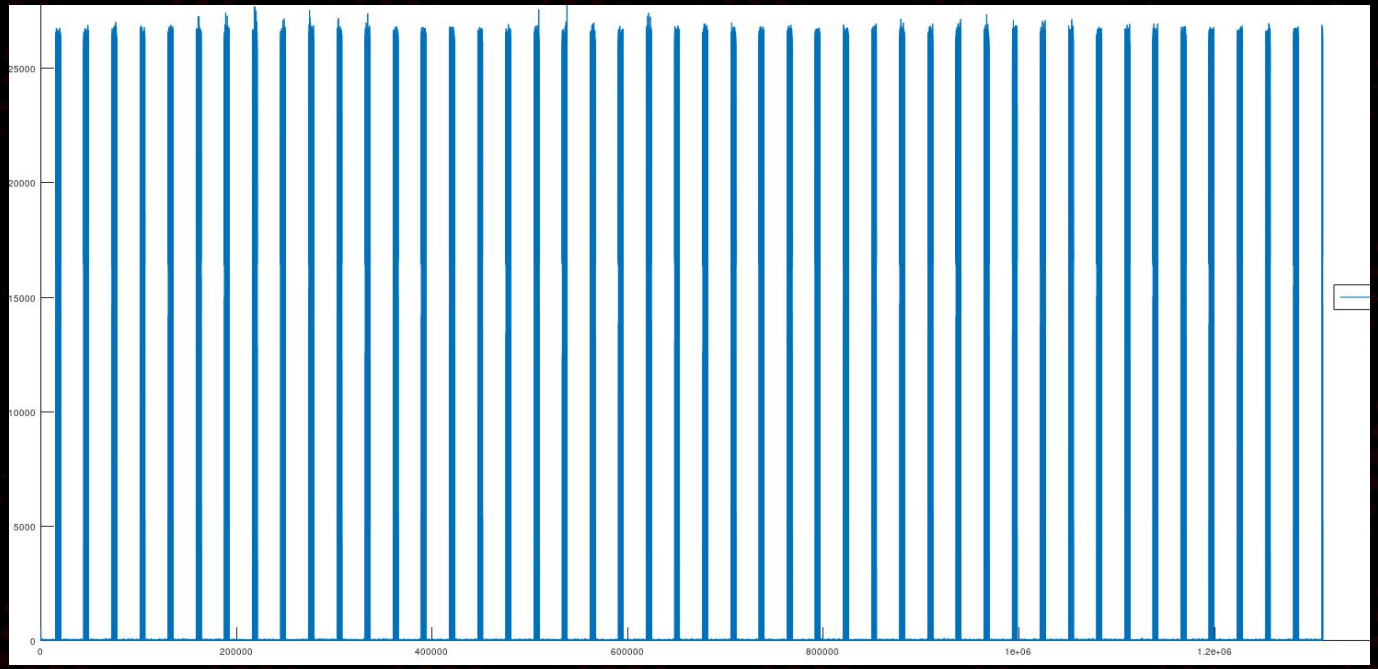
2ASK

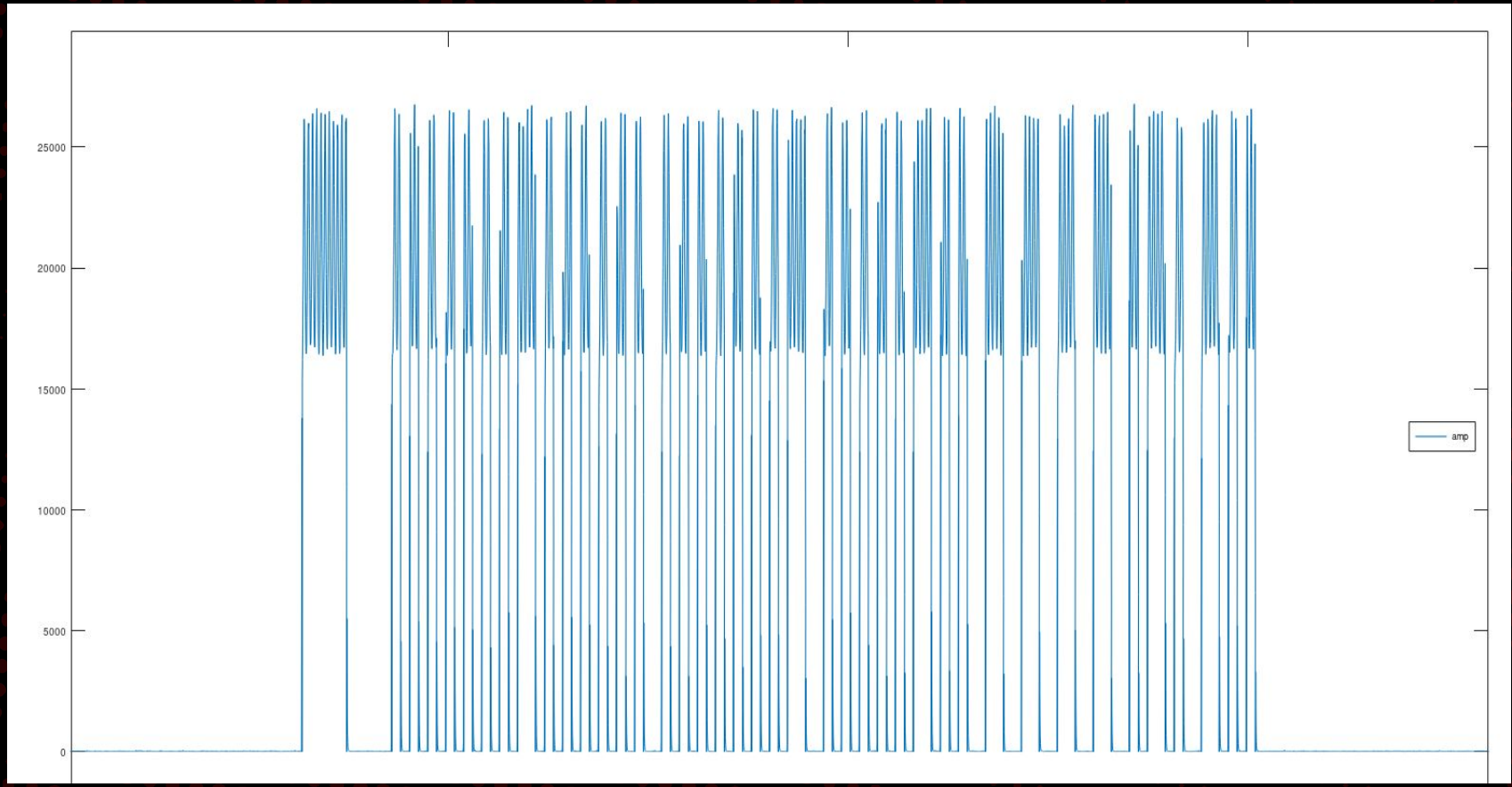


In-phase / Quadrature






25000
20000
15000
10000
5000
0
0
200000
400000
600000
800000
1e+06
1.2e+06


25000
20000
15000
10000
5000
0
amp

Custom Driver for I2S de MT7628

- ➤ Accepts bit stream from a dev file (/dev/fh_ss)
- ➤ Modulates in “2ASK”. Adds CRC8
- ➤ TWO hrtimers. One for symbol generation and the other one for packet timed synced generation



RECEIVER: Another Vocore2, with SDR

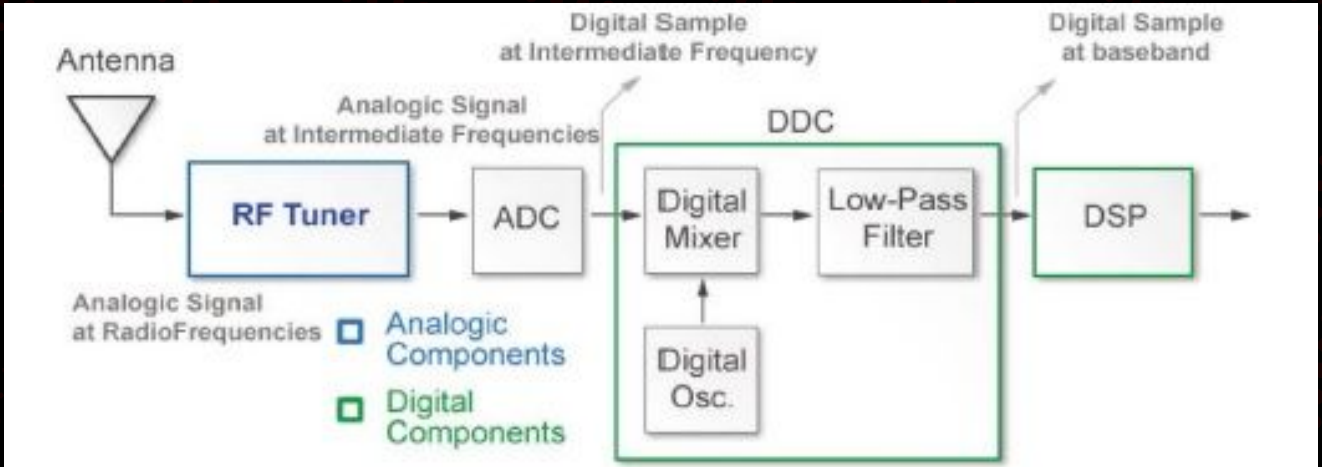
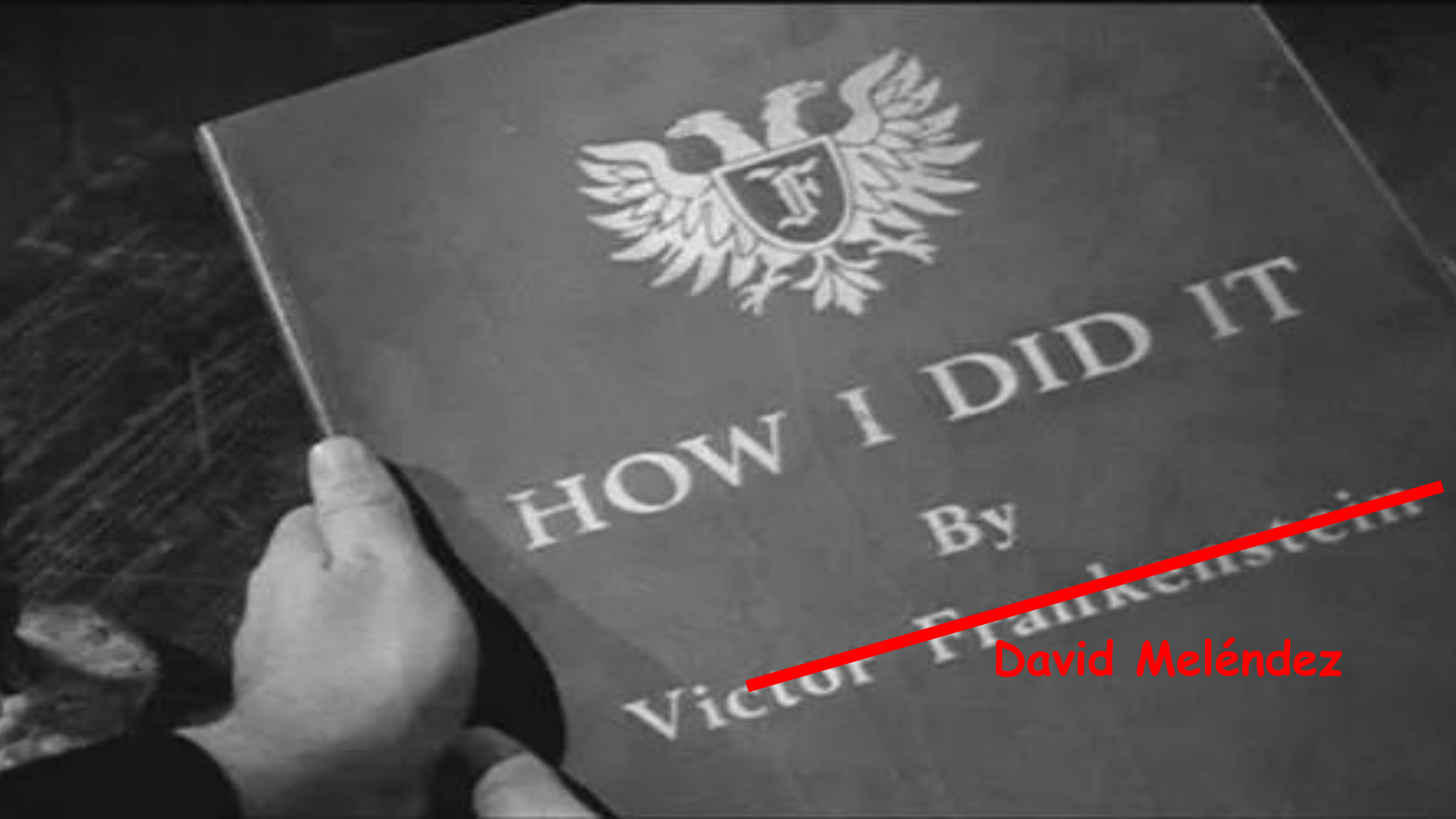


FIG. 2. Block Diagram of the SDR Receiver.


HOW I DID IT
By
Victor Frankenstein
David Meléndez

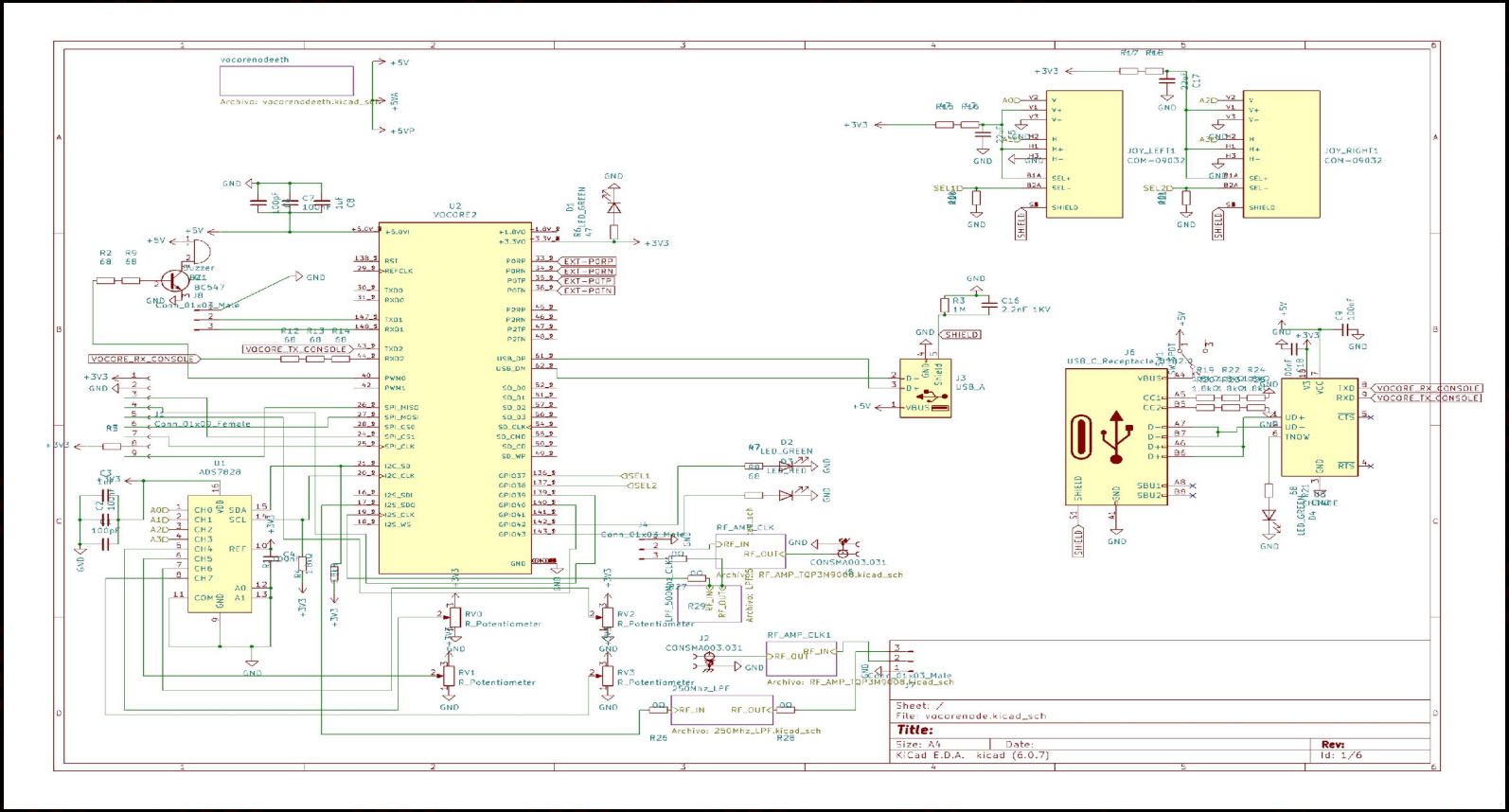
SDR: Frequency hopping

- Requires reiterative calls to librtlsdr

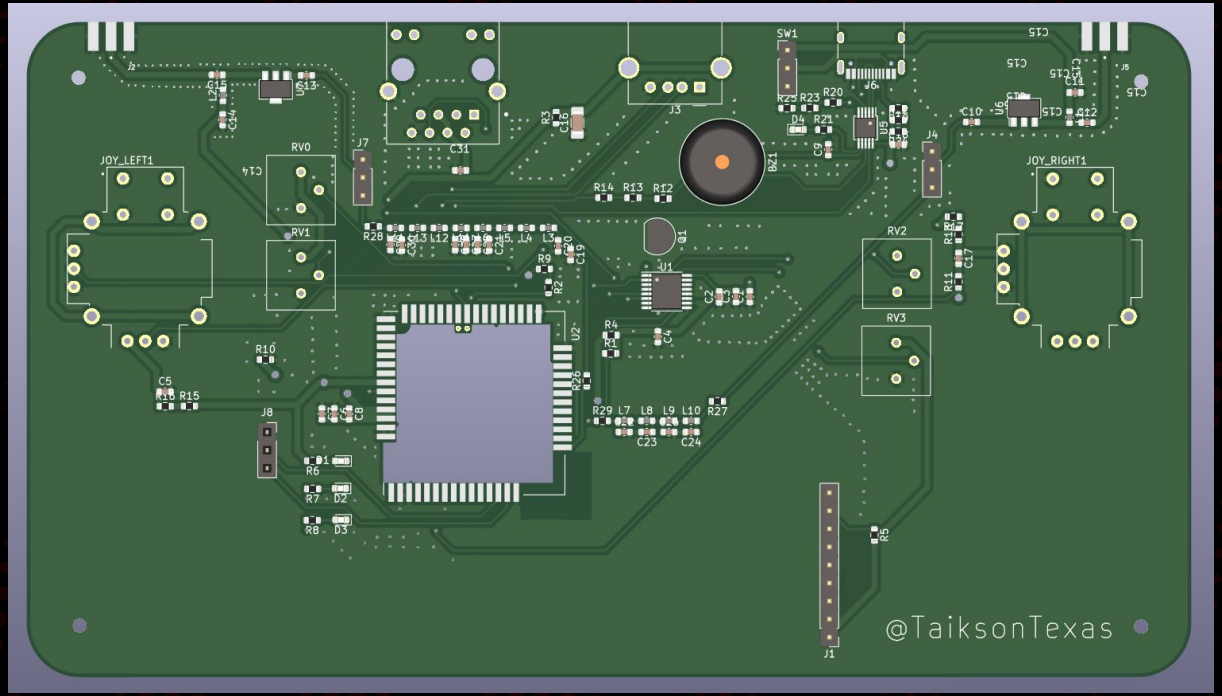
```
rtlsdr_set_center_freq(dev, divisor_to_freq_hz(_divisors_fhss[0]));
```

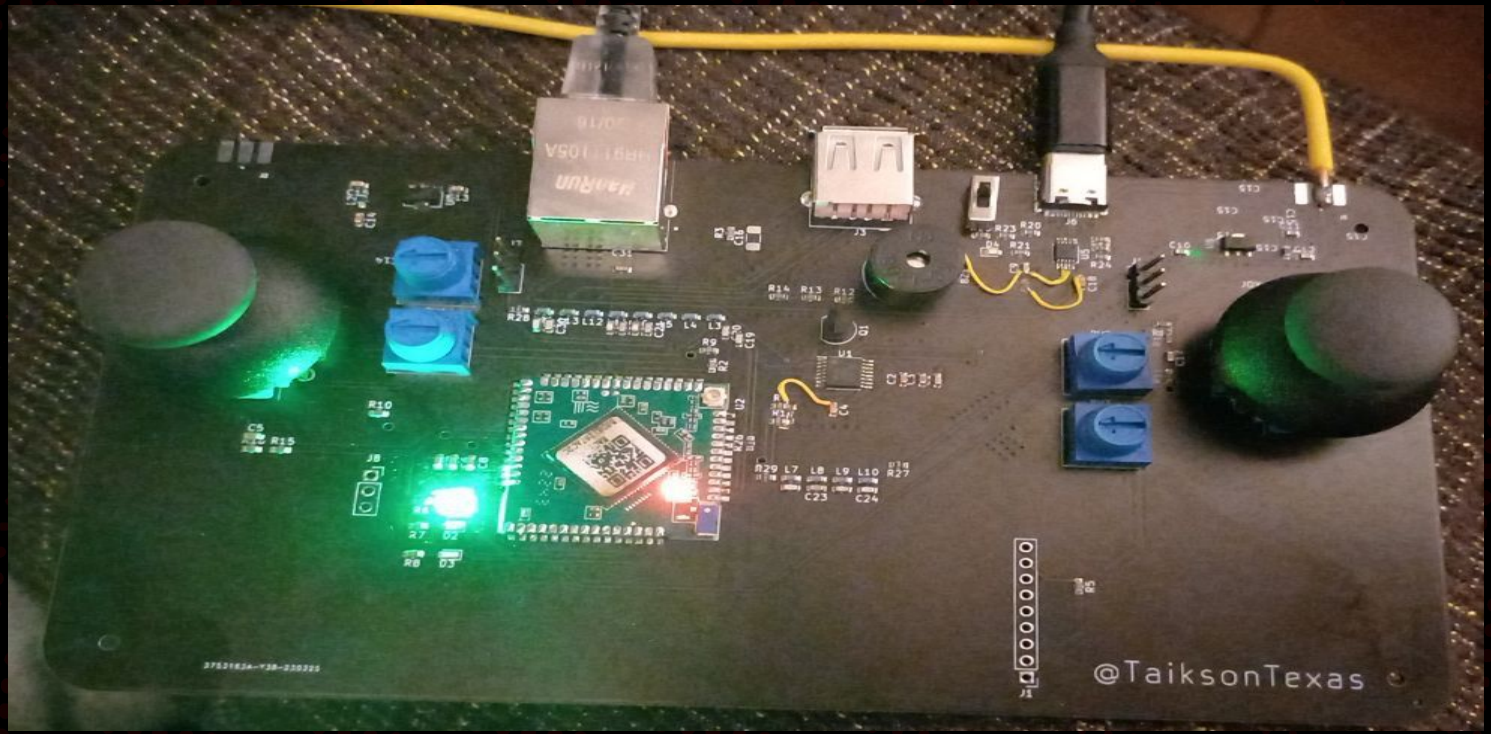
- Synchronization with pregenerated and preshared list of frequencies.

Custom controller with all components:



Custom controller with all components:




@TaiksonTexas

Next episode: DSSS

Thanks!



@TAIKSONTEXAS





@CONSTRAINTERROR