Project “The Interceptor”:

Owning anti-drone systems with nanodrones

David Meléndez Cano
R&D Embedded Systems Engineer


@taiksontexas

David Meléndez Cano

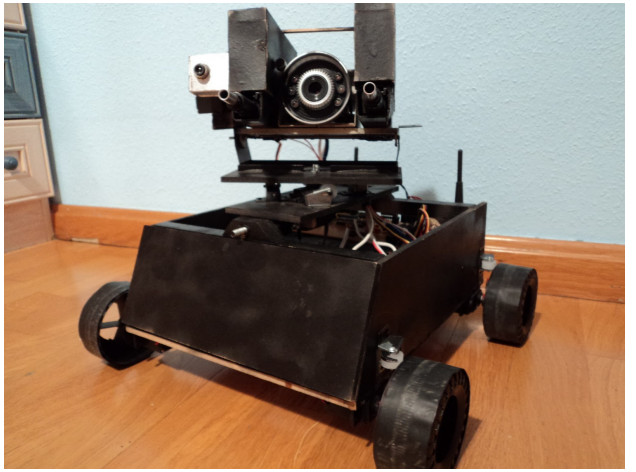


@TaiksonTexas

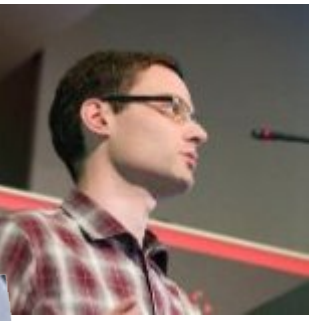
- *R&D Embedded Software Engineer in Albalá Ingenieros, S.A. Spain*
- *Author of the robots: "Atropos" & "Texas Ranger"*
- *Author of the Book "Hacking con Drones"*
- *"Reincident" speaker*
- *Trainiac*





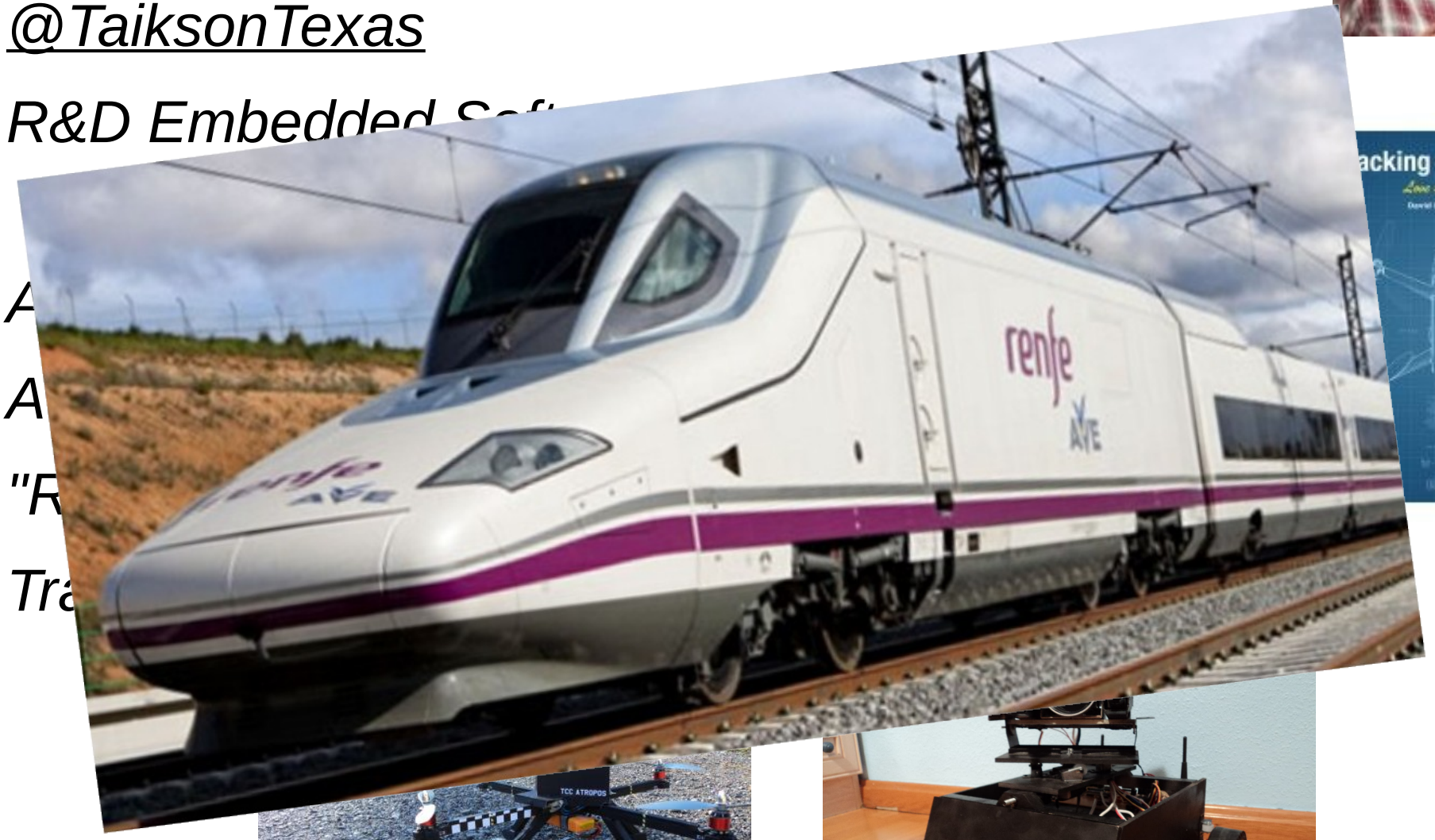


David Meléndez Cano



@TaiksonTexas

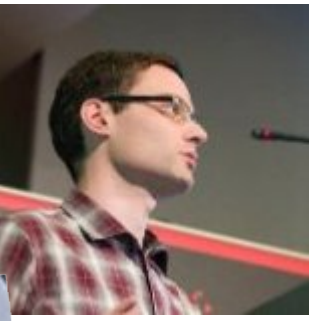
- *R&D Embedded Soft*
- *A*
- *A*
- *"R*
- *Tra*







David Meléndez Cano



@Taik

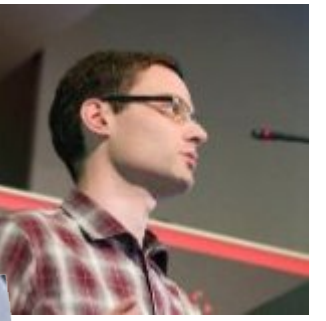
- *R&D*
- *A*
- *A*
- *"R*
- *Tr*







David Meléndez Cano



@Taik

- *R&D*
- *A*
- *A*
- *"R*
- *Tr*







US & WORLD \ TECH \ NATIONAL SECURITY

A US ally shot down a $200 drone with a $3 million Patriot missile

This will be a bigger problem as more drones show up on the battlefield

by Andrew Liptak | @AndrewLiptak | Mar 16, 2017, 10:13am EDT

SHARE TWEET LINKEDIN



NOW TRENDING



Previously in DEFCON...



@taiksontexas

Previously in DEFCON...

Blighter - AUDS (Anti-UAV Defence System) – Detect, Track, Disrupt, Defeat
- http://www.blighter.com/products/auds-anti-uav-defence-system.html

69

Defeating Jammers

HACKING PERIPHERALS – CELLULAR 3G USB & GPS – SECURE COMMAND & CONTROL



- Remote control over SSH tunnel via 3G USB cell connection. GPS & Cellular signals are illegal to jam (see FCC regulations), making it hard to defend against this type of drone.
  - https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf



Attacker



Mission Planner





Cell Tower



Cell Tower



Target Building

Wireless / Bluetooth / ZigBee / etc. Pen Testing





70

- Note: be sure to check upcoming FCC regulations about needing to keep drone within line of sight while flying.

@taiksontexas

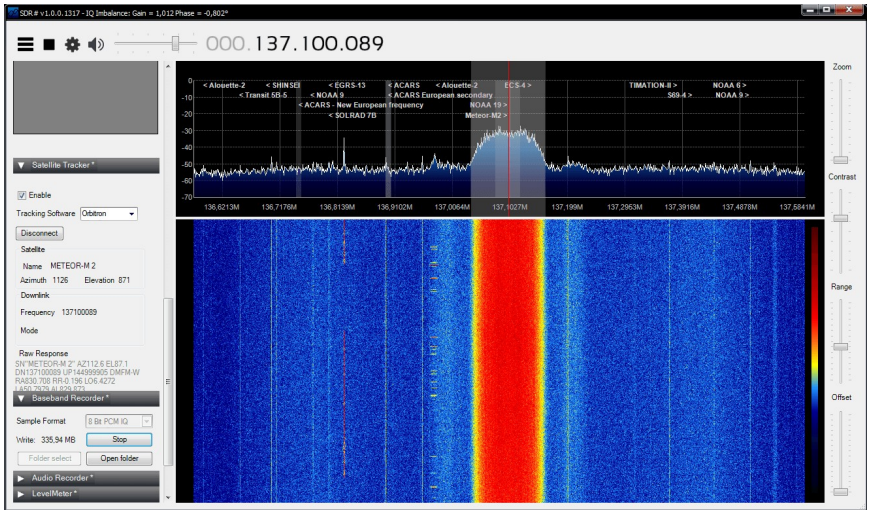
Drones as a threat

- Flying computers. *(IoT over your head.)*
- Custom payloads:
  - Sniffers
  - Jammers
  - Network Analyzers
  - 3d mapping, cameras.
  - Physical attacks, explosives.
  - ...



Detection

- Thermal and standard cameras
  - A.I. to detect drone shape
  - Electronics and motor heat detection
- Characterization of drone noise
- **Detected Radio Frequency and waveform**
  - Radio signature



“Voluntary” measures

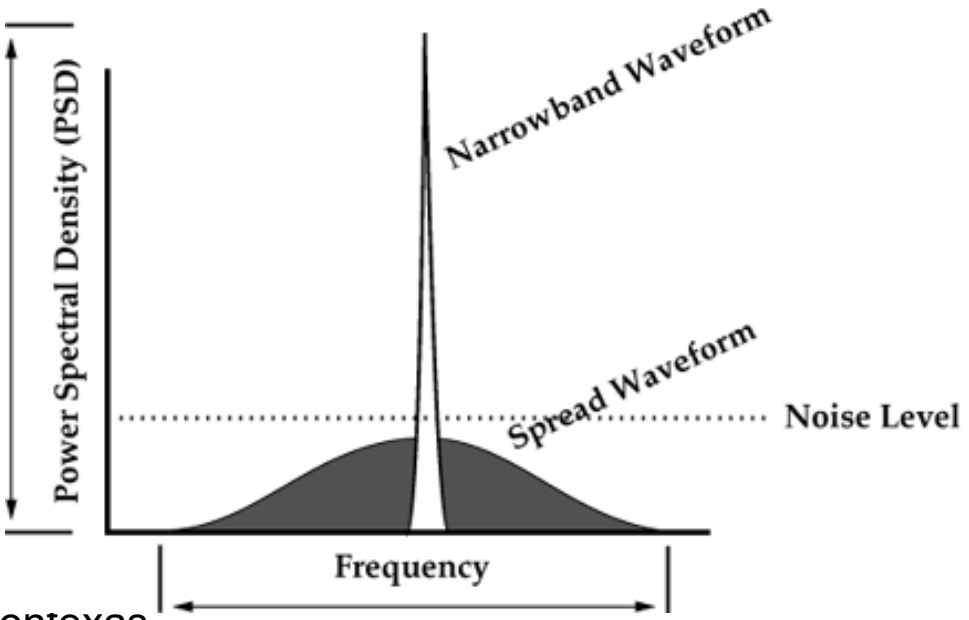


- No-fly zone controlled by onboard GPS and Autopilots
- Real time telemetry transmission to COPS
- Give to COPS the ability to take down your drone and “*everything will be alright*”

Counter-Countermeasures

- Spread-spectrum
- Frequency hopping
- Use unespected frequencies by the jammer
- Robust protocols





First Round: “**ATROPOS**”

Dron **ATROPOS**

- WiFi Router
- PIC16F876 for PWM
- Wii Nunckuck and Motion + as onboard IMU
- HTML5 telemetry by router webserver
- WiFi comm.
- WPS Attacks with bully

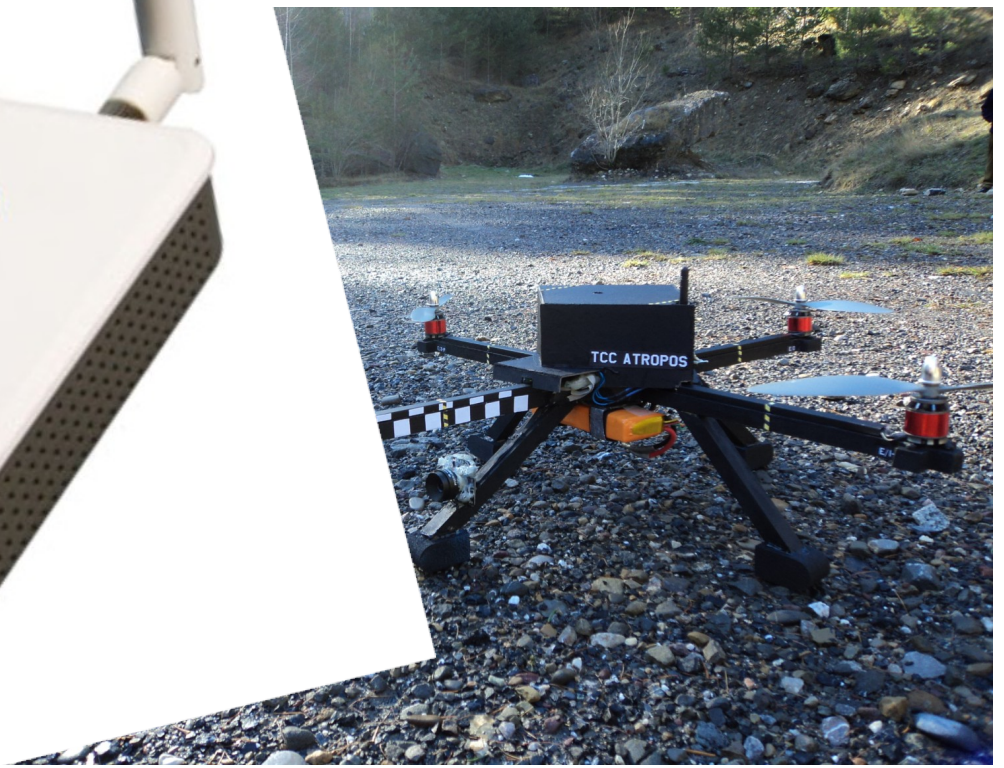


First Round: “**ATROPOS**”

Dron **ATR**

- WiFi
- PIC1
- Wii Nu
  Motion
- HTML5
  webserv
- WiFi com
- WPS Attac

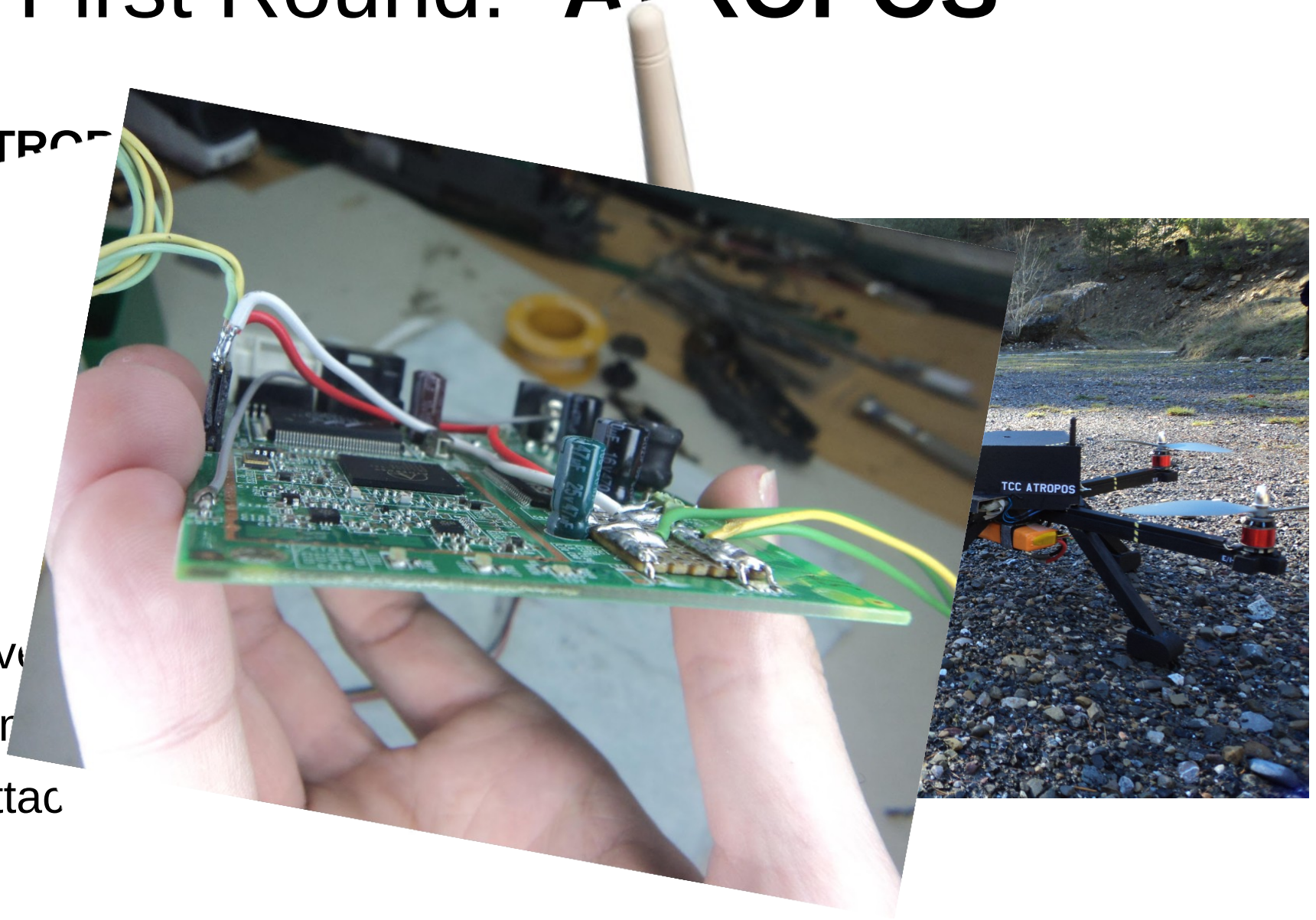




First Round: “**ATROPOS**”

Dron **ATRO**

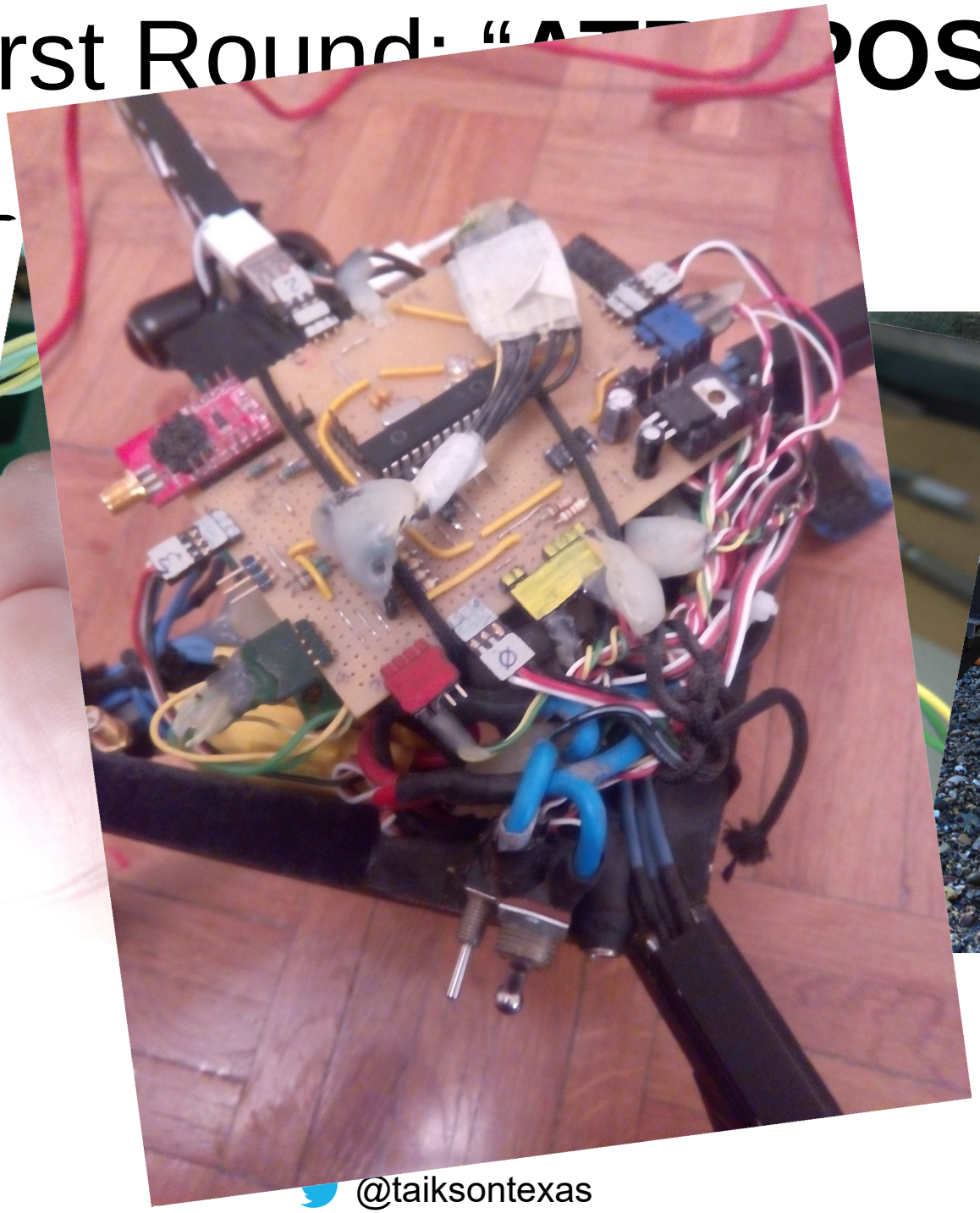
- WiFi
- PIC1
- Wii Nu
  Motion
- HTML5
  webserv
- WiFi cor
- WPS Attac



First Round: "ATROPOS"

Dron **ATRO**

- WiFi
- PIC1
- Wii Nu
  Motion
- HTML5
  webserv
- WiFi cor
- WPS Attac





Now, what else?

“We count thirty Rebel ships, Lord Vader…



…but they're so small they're evading our turbolasers”

@taiksontexas

Project “***The Interceptor***”

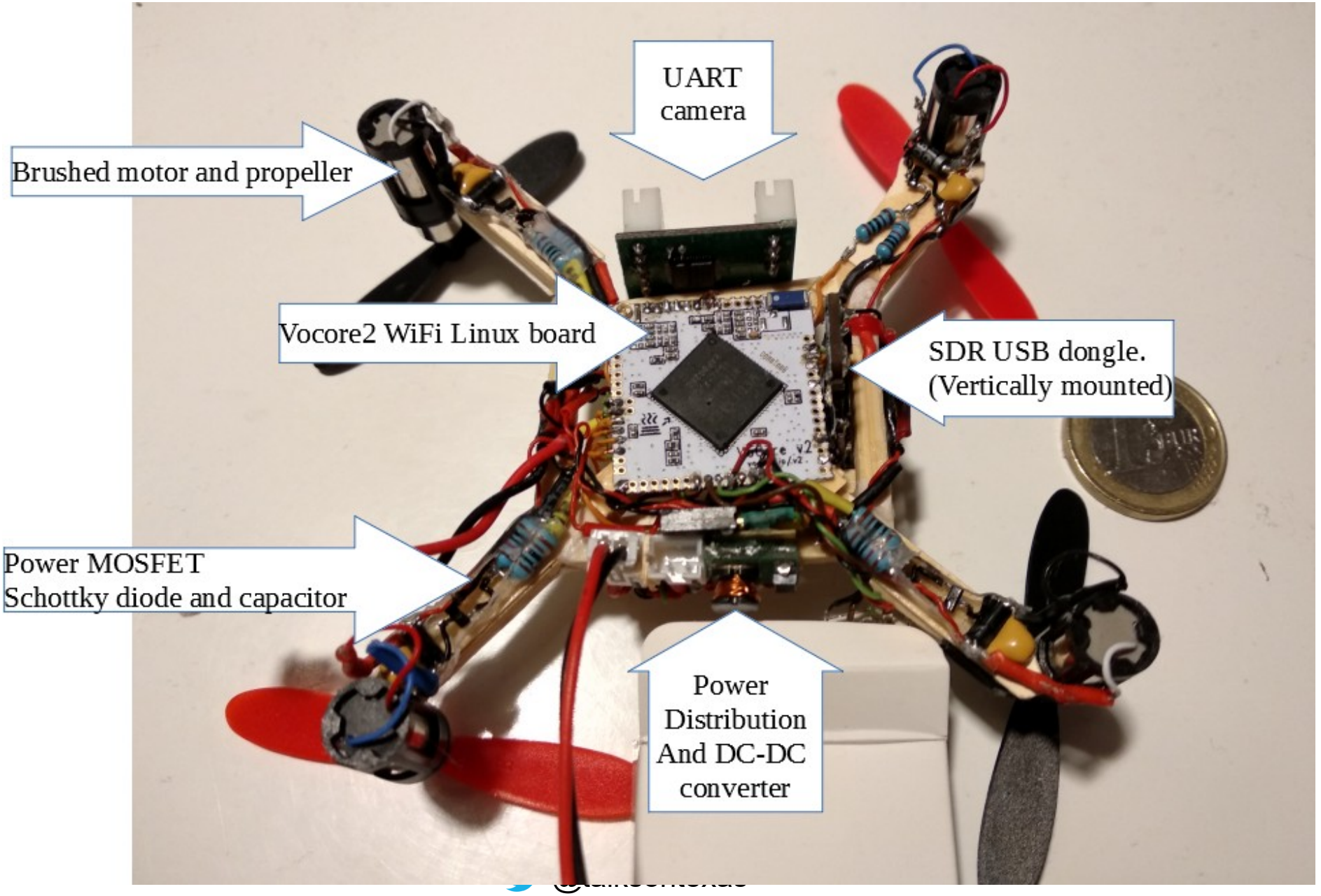


Project "*The Interceptor*"

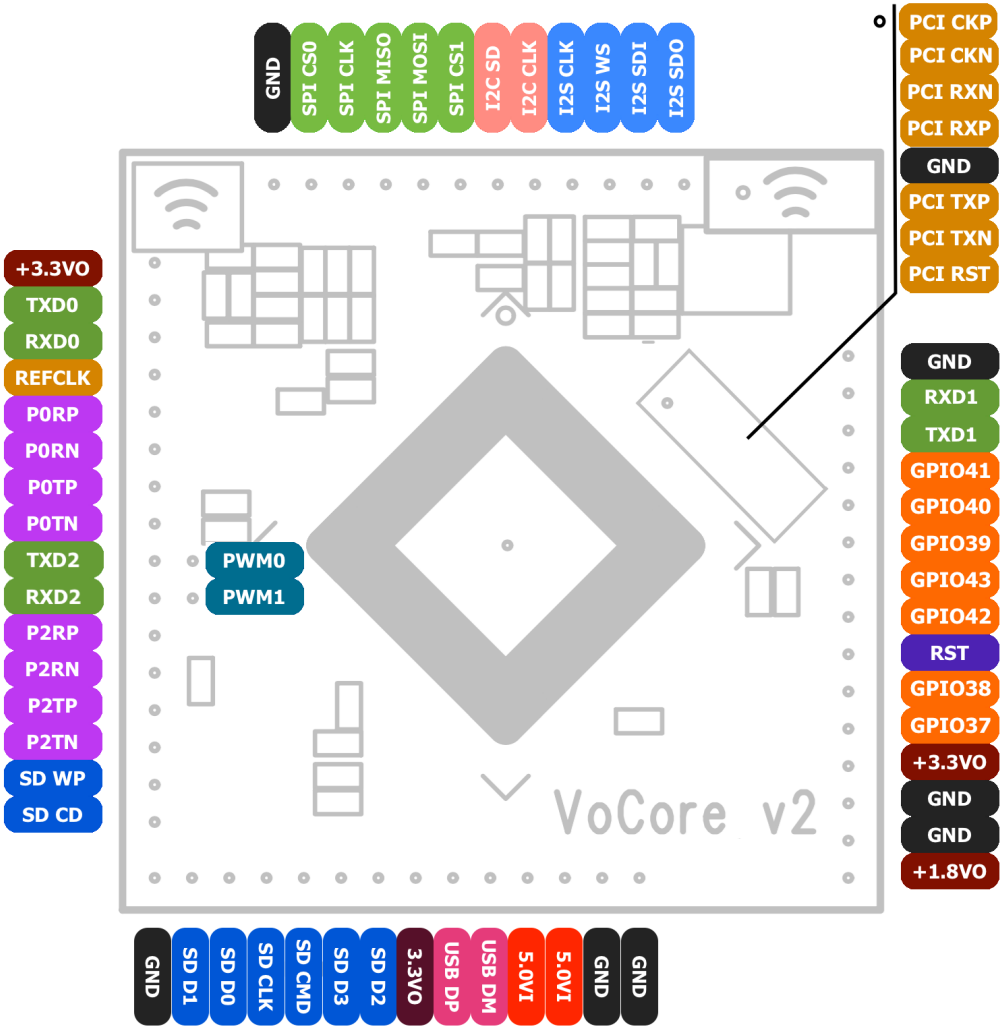
- Minimum size and weight (harder to detect)
- Low budget *(no, seriously, really low)*

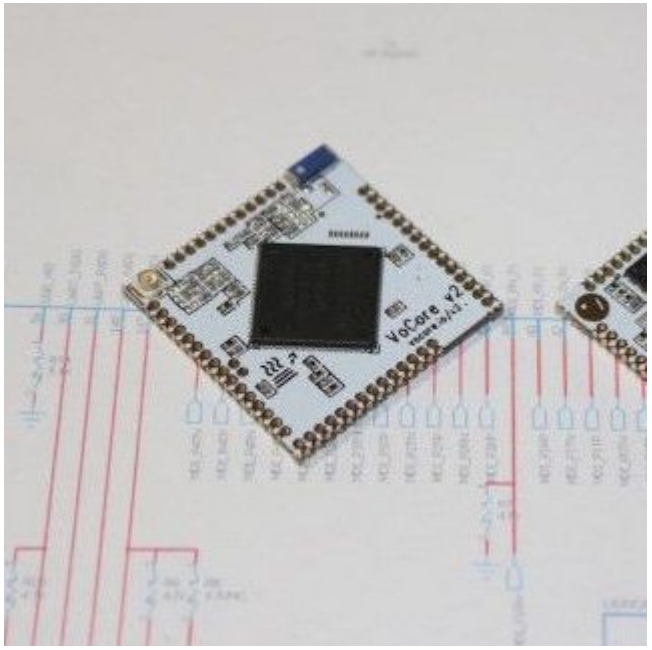
  ~$40 + $20 with SDR
- Hacking capabilities
- "Resilient" control

Project "*The Interceptor*"



Vocore2





@taiksontexas

Vocore2

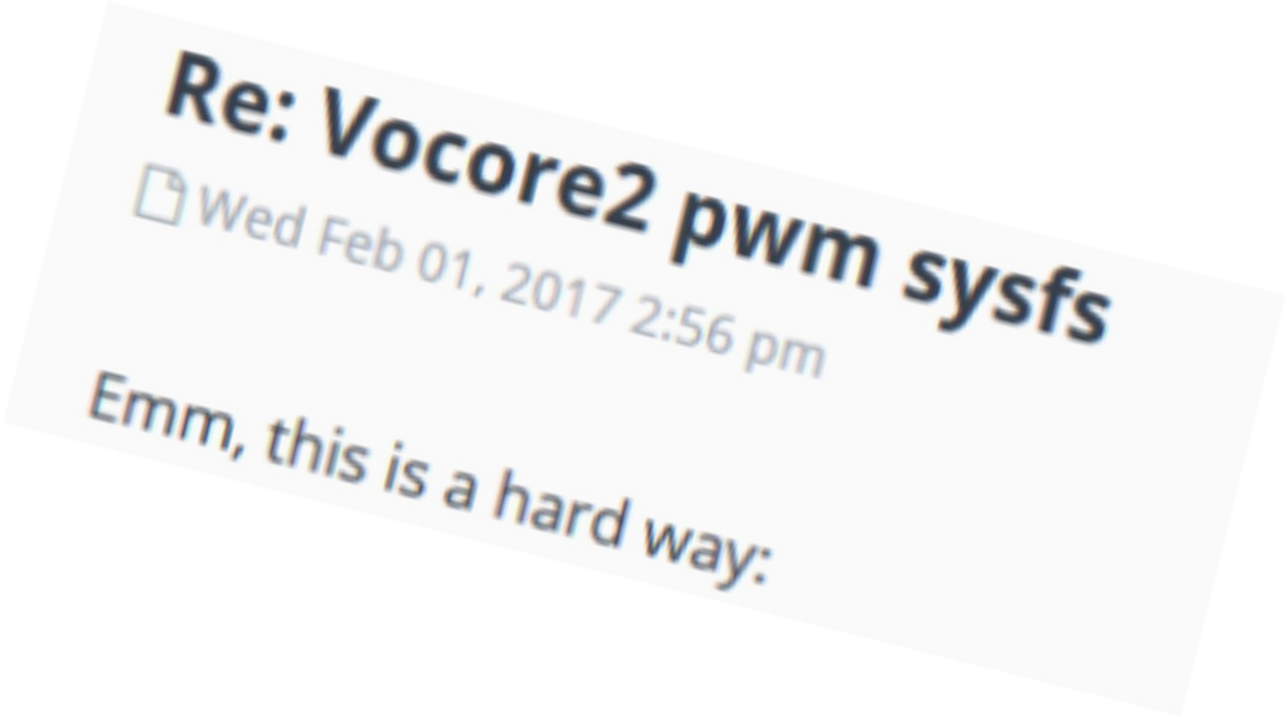
Parameters

	Details
SIZE	25.6mm x 25.6mm x 3.0mm
CPU	MT7628AN, 580 MHz, MIPS 24K
MEMORY	128MB, DDR2, 166MHz
STORAGE	16M NOR on board, support SDXC up to 2TB
WIRELESS	802.11n, 2T2R, speed up to 300Mbps.
ANTENNA	One U.FL slot, one on board antenna.
ETHERNET	1 port/5 ports, up to 100Mbps.
USB	Support USB 2.0, up to 480MBit/s.
PCIe 1.1	Supported
GPIO	>=40 (pinmux)
UART	x3 (UART2 for debug console)
PWM	x4
POWER SUPPLY	3.6V ~ 6.0V, 500mA
POWER CONSUMPTION	74mA wifi standby, 230mA wifi full speed, 5V input.

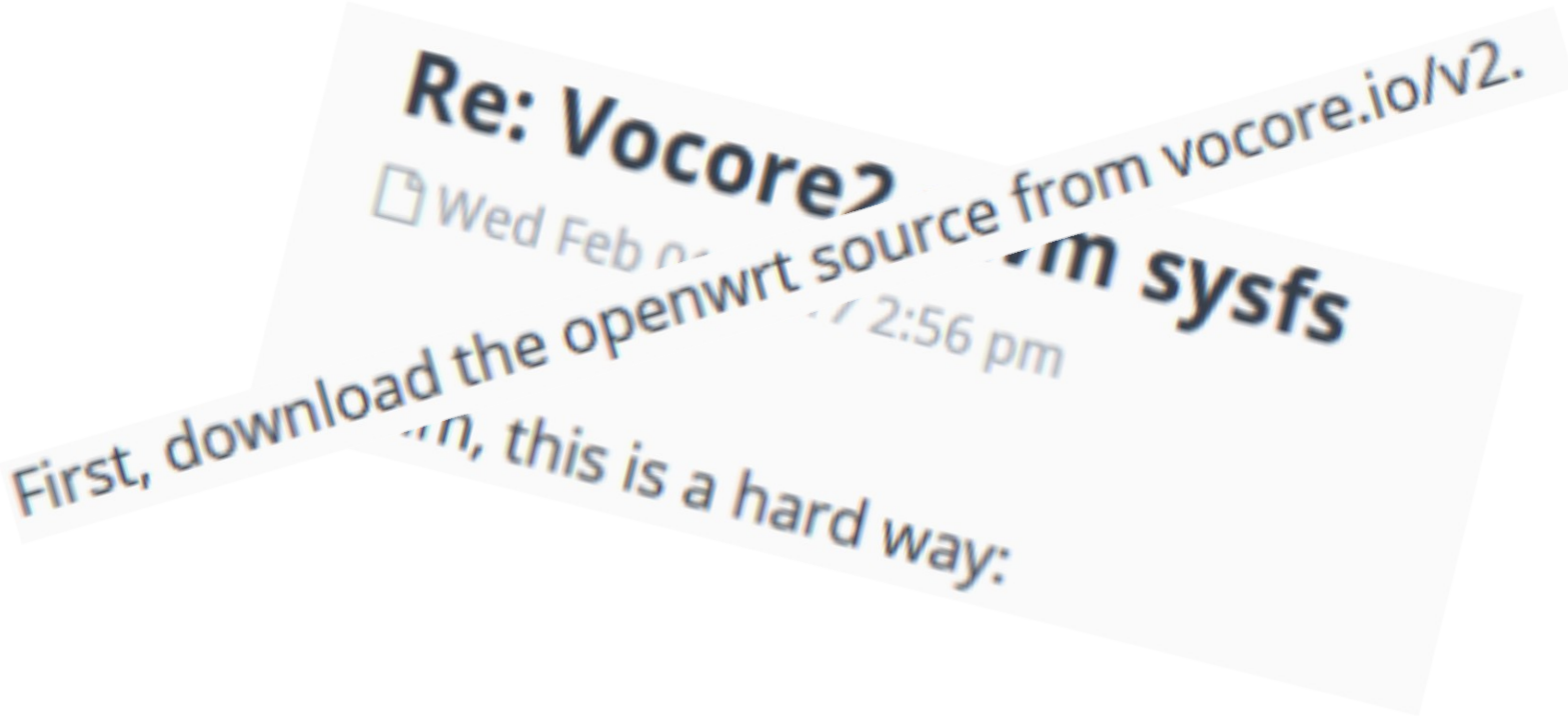
Vocore2: PWM

- We need to generate x4 PWM signals to control the motors
  - Hard real time constrained. Need specific HW.
- x4 channels available, but only 2 enabled
- Last two overlap with UART2 function
  - Disable UART2 in devicetree
  - Enable PWMx4 in devicetree

Vocore2: PWM in the forum

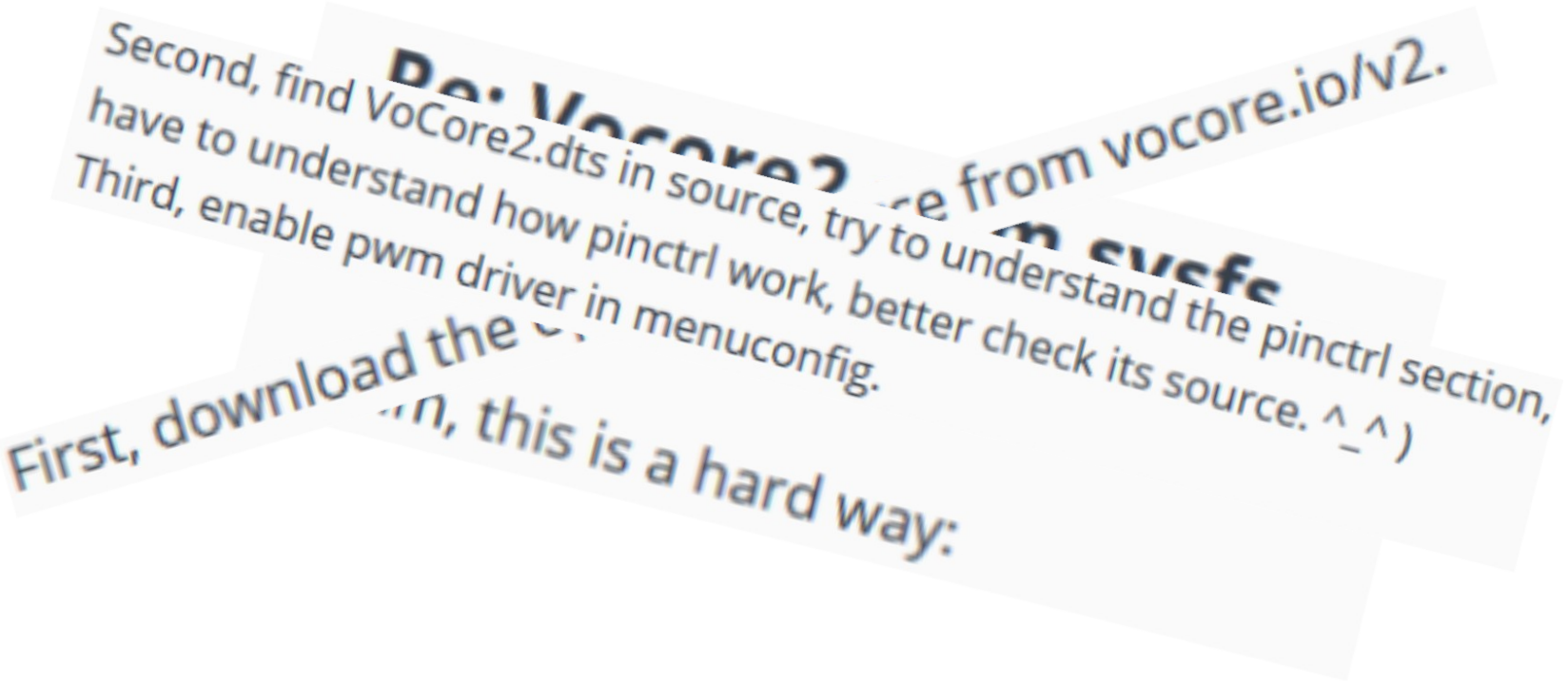


Vocore2: PWM in the forum

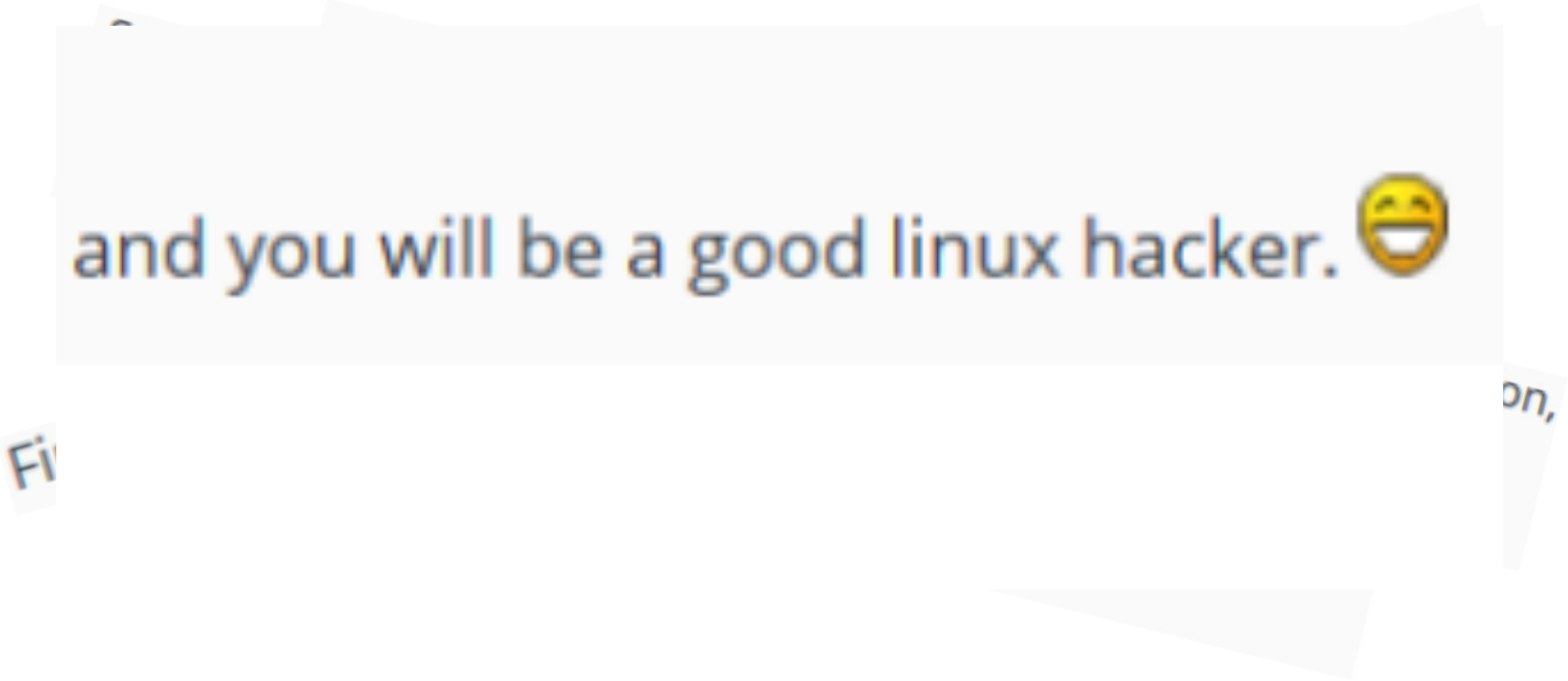


@taiksontexas

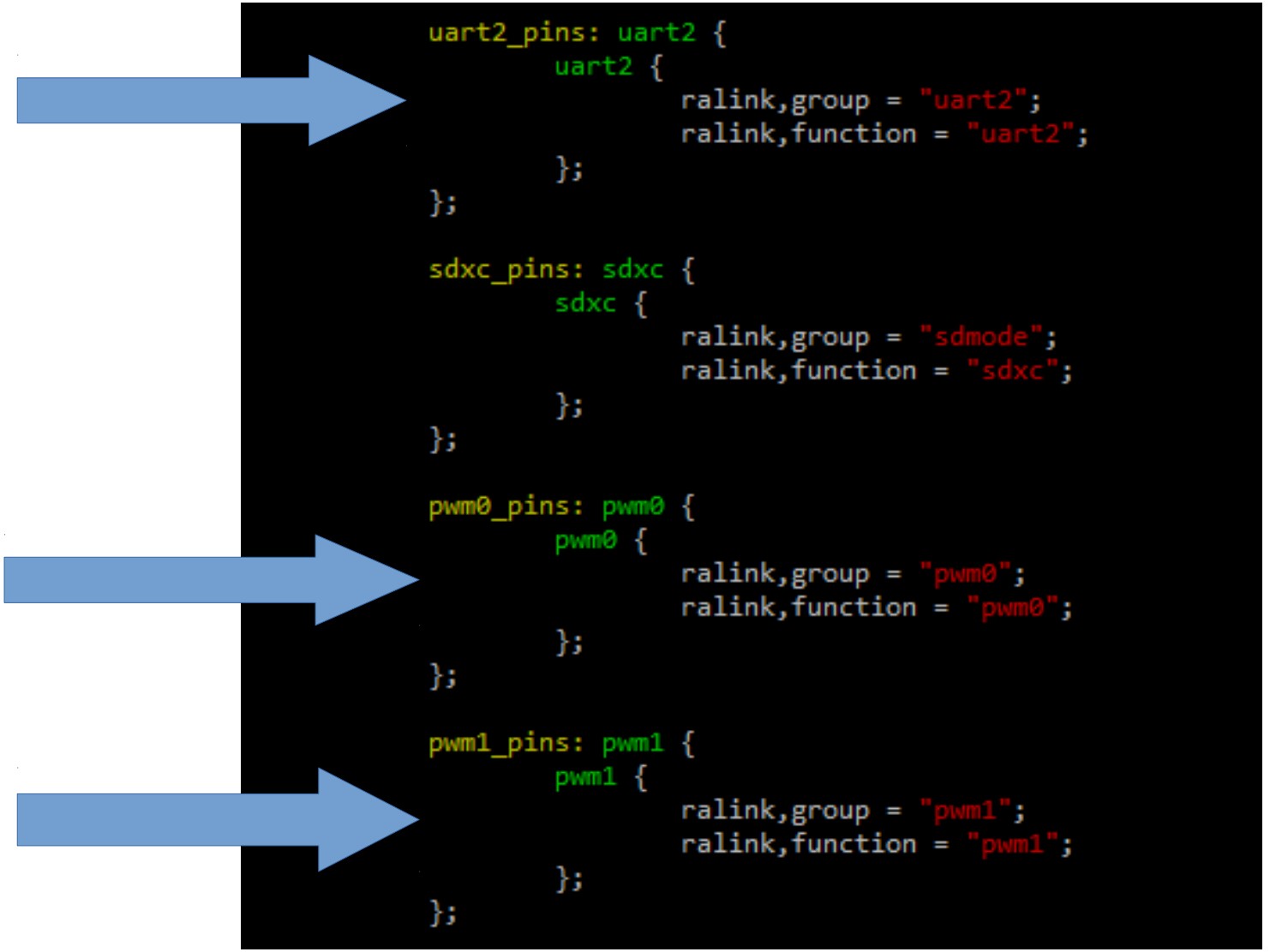
Vocore2: PWM in the forum



Vocore2: PWM in the forum



Vocore2: PWM (pinmux)



```
uart2_pins: uart2 {
        uart2 {
                ralink,group = "uart2";
                ralink,function = "uart2";
        };
};

sdxc_pins: sdxc {
        sdxc {
                ralink,group = "sdmode";
                ralink,function = "sdxc";
        };
};

pwm0_pins: pwm0 {
        pwm0 {
                ralink,group = "pwm0";
                ralink,function = "pwm0";
        };
};

pwm1_pins: pwm1 {
        pwm1 {
                ralink,group = "pwm1";
                ralink,function = "pwm1";
        };
};
```

./target/linux/ramips/dts/mt7628an.dtsi

Vocore2: PWM (pinmux)

Pinmux redefinition

ADC chip declaration
Present in I2C for battery

Disabled UART2

Enabled all 4 PWM

```
&pinctrl {

        pwm_pins: pwm{
                pwm0{
                        ralink,group = "pwm0";
                        ralink,function = "pwm0";
                };
                pwm1{
                        ralink,group = "pwm1";
                        ralink,function = "pwm1";
                };
                uart2_pwm{
                        ralink,group = "uart2";
                        ralink,function = "pwm";
                };
        };

};
&i2c{
        status = "okay";
        clock-frequency = <400000>;

        adc@0 {
                compatible = "microchip,mcp3426";
                reg = <0x68>;
        };
};


&uart2 {
        status = "disabled";
        //status= "okay";
};


&pwm {
        pinctrl-0 = <&pwm_pins>;
        status="okay";
        //status="disabled";

};
```

Vocore2: pinmux mt7628 (datasheet)

3.3.18 UART2 pin share scheme

Controlled by the EPHY_APGIO_AIO_EN[4:1] and UART2_MODE registers

	4'b0000	4'b1111			
Pin Name		**2'b00**	**2'b01**	**2'b10**	**2'b11**
MDI_TP_P2	MDI_TP_P2	UART_TXD2	GPIO#20	PWM_CH2	eMMC_D5
MDI_TN_P2	MDI_TN_P2	UART_RXD2	GPIO#21	PWM_CH3	eMMC_D4

3.3.19 PWM_CH0 pin share scheme

Controlled by the EPHY_APGIO_AIO_EN[4:1] and PWM0_MODE registers

	4'b0000	4'b1111			
Pin Name		**2'b00**	**2'b01**	**2'b10**	**2'b11**
MDI_RP_P2	MDI_RP_P2	PWM_CH0	GPIO#18		eMMC_D7

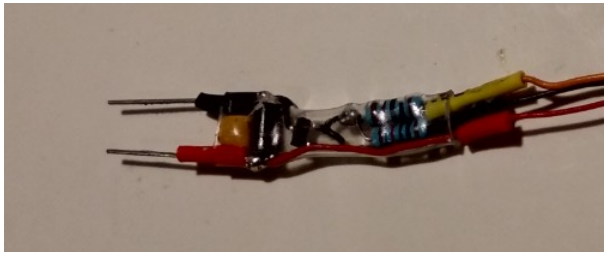
3.3.20 PWM_CH1 pin share scheme

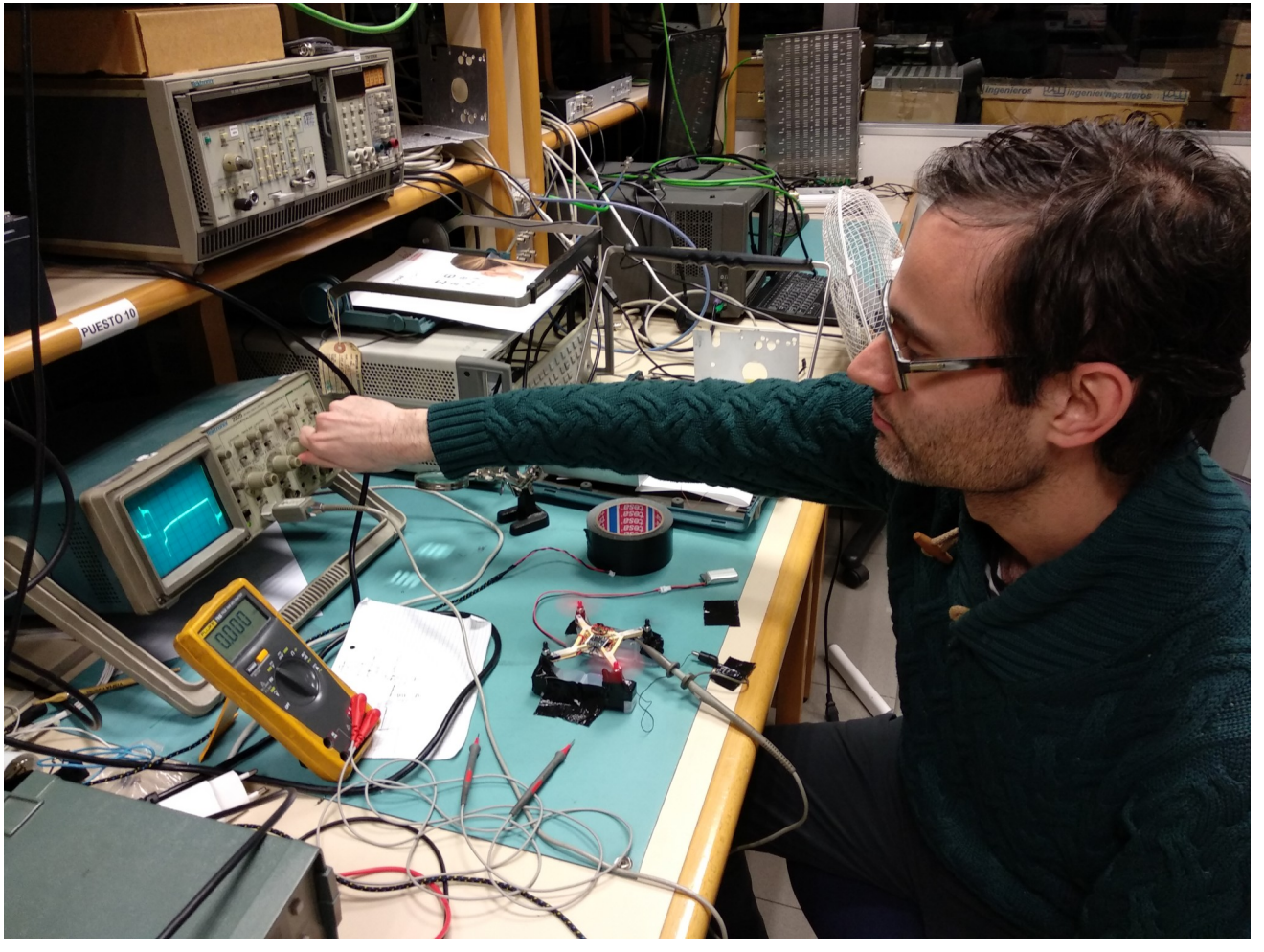
Controlled by the EPHY_APGIO_AIO_EN[4:1] and PWM1_MODE registers

	4'b0000	4'b1111

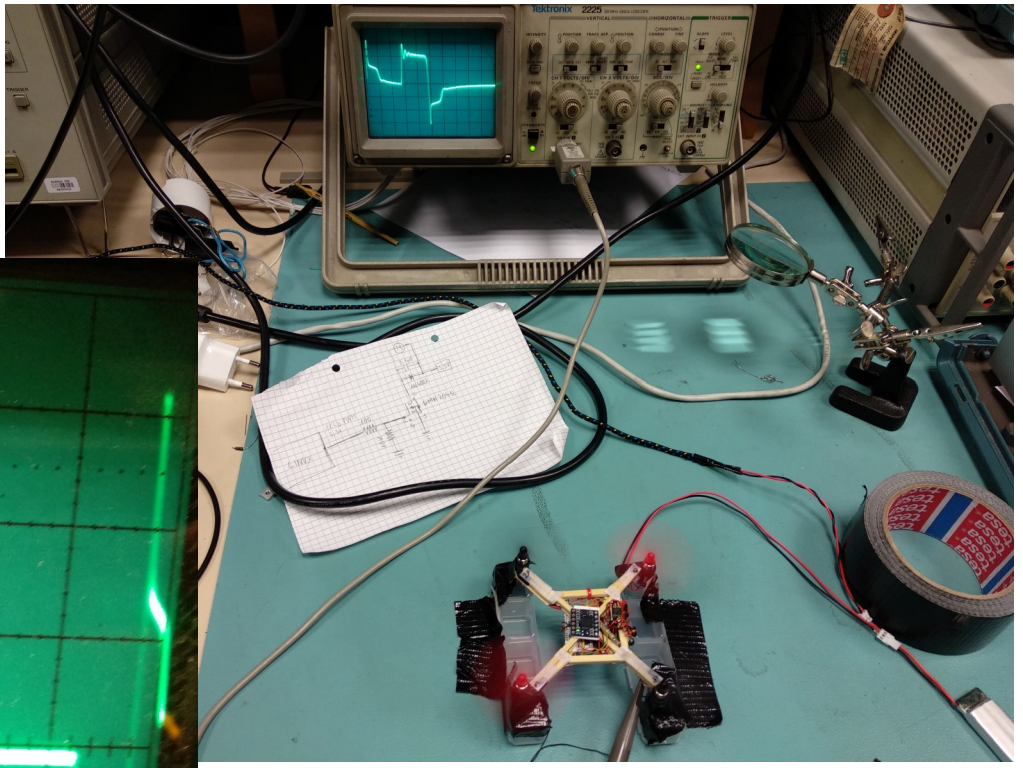
Power stage

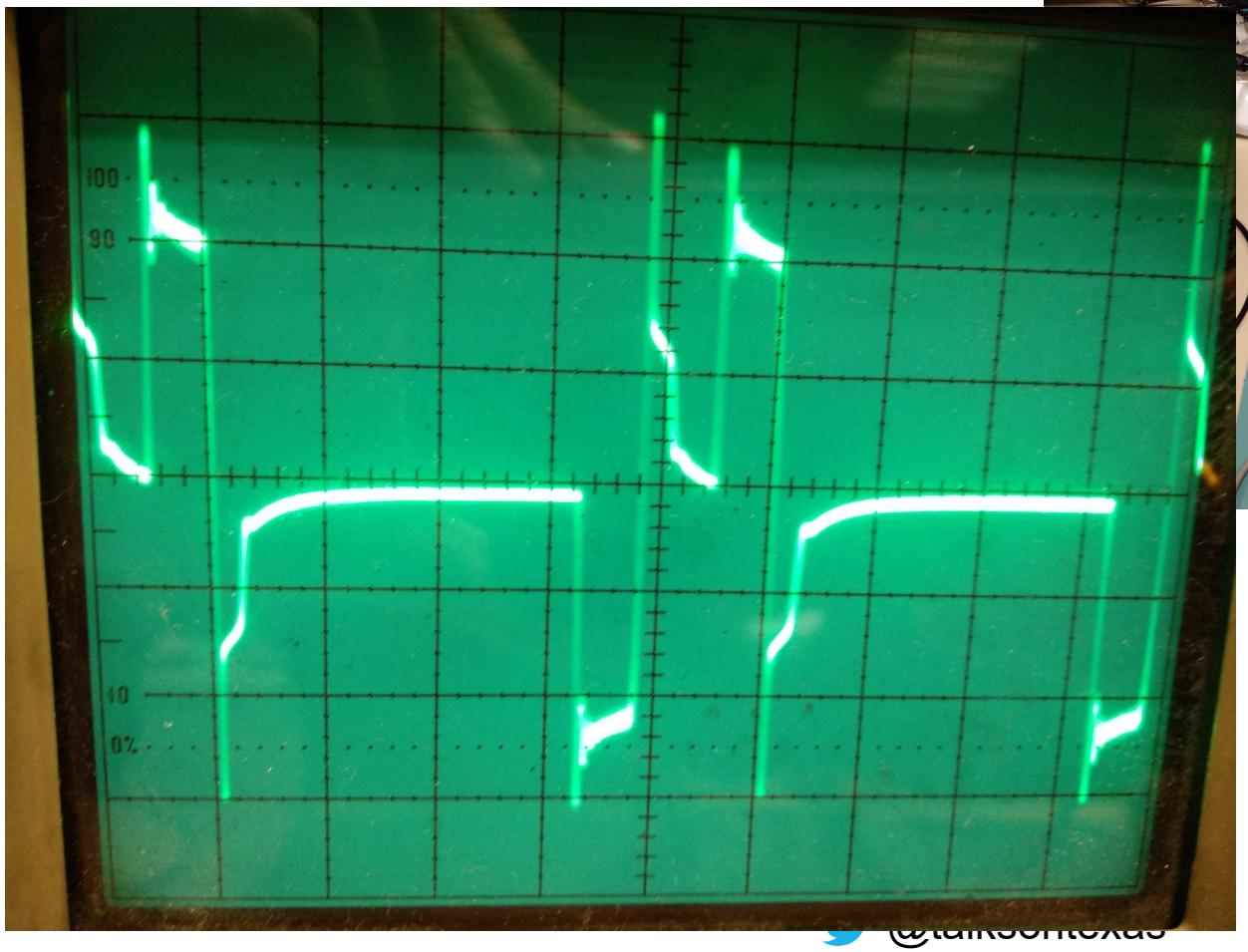
- Brushed motors (cheap as hell)
- X1 MOSFET
- X1 Capacitor
- X1 Schottky diode



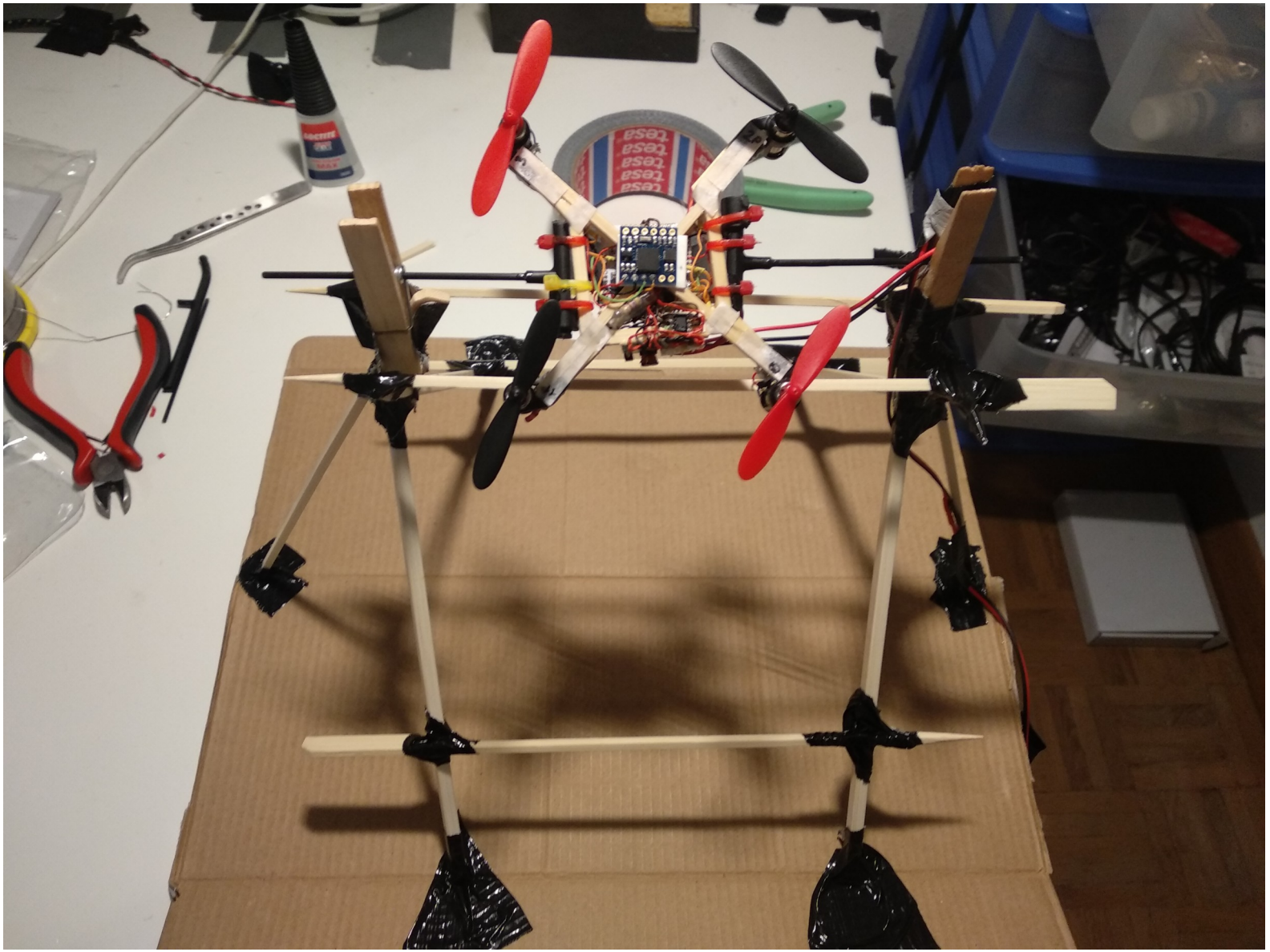


Electrical motor behaviour



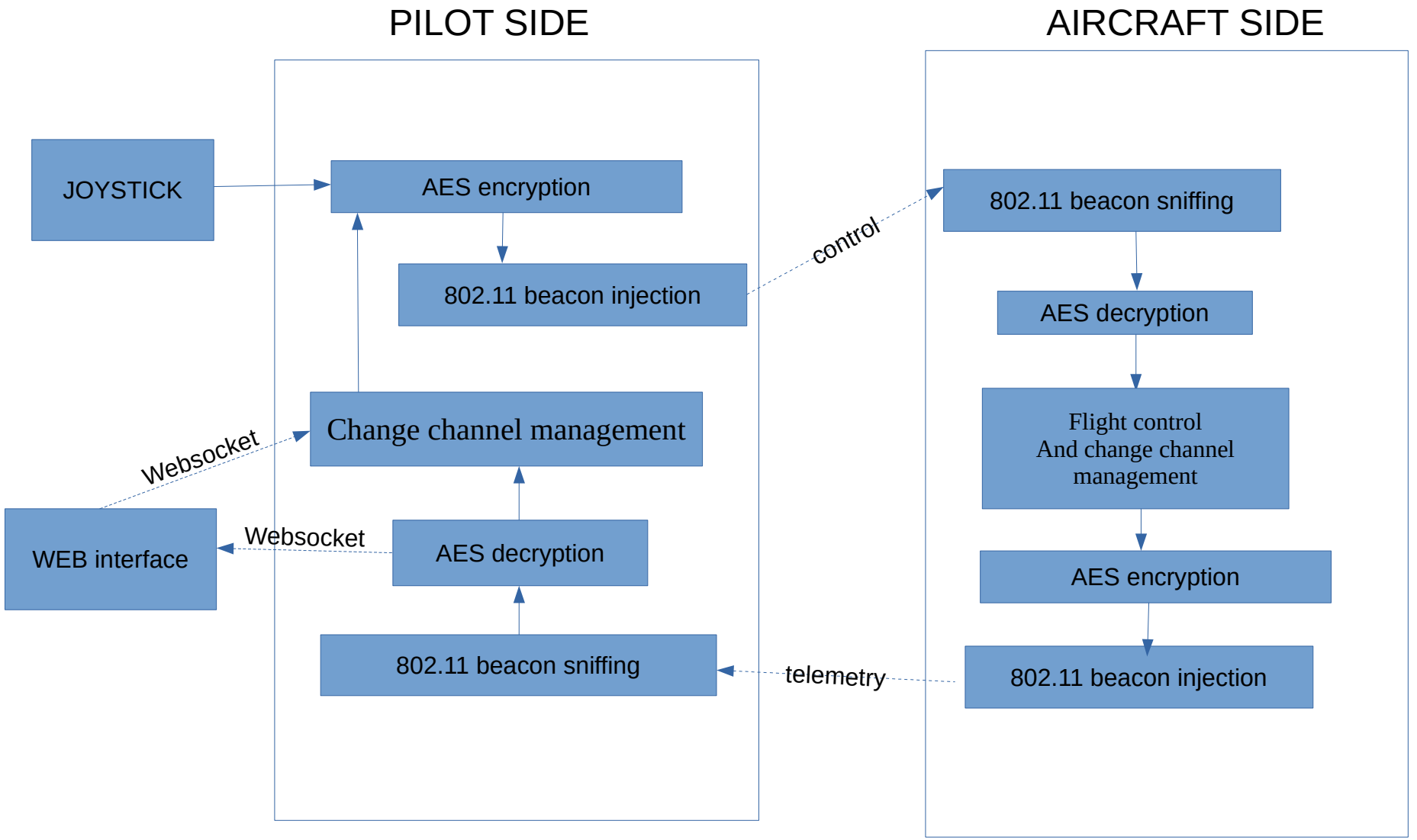


PID tunning



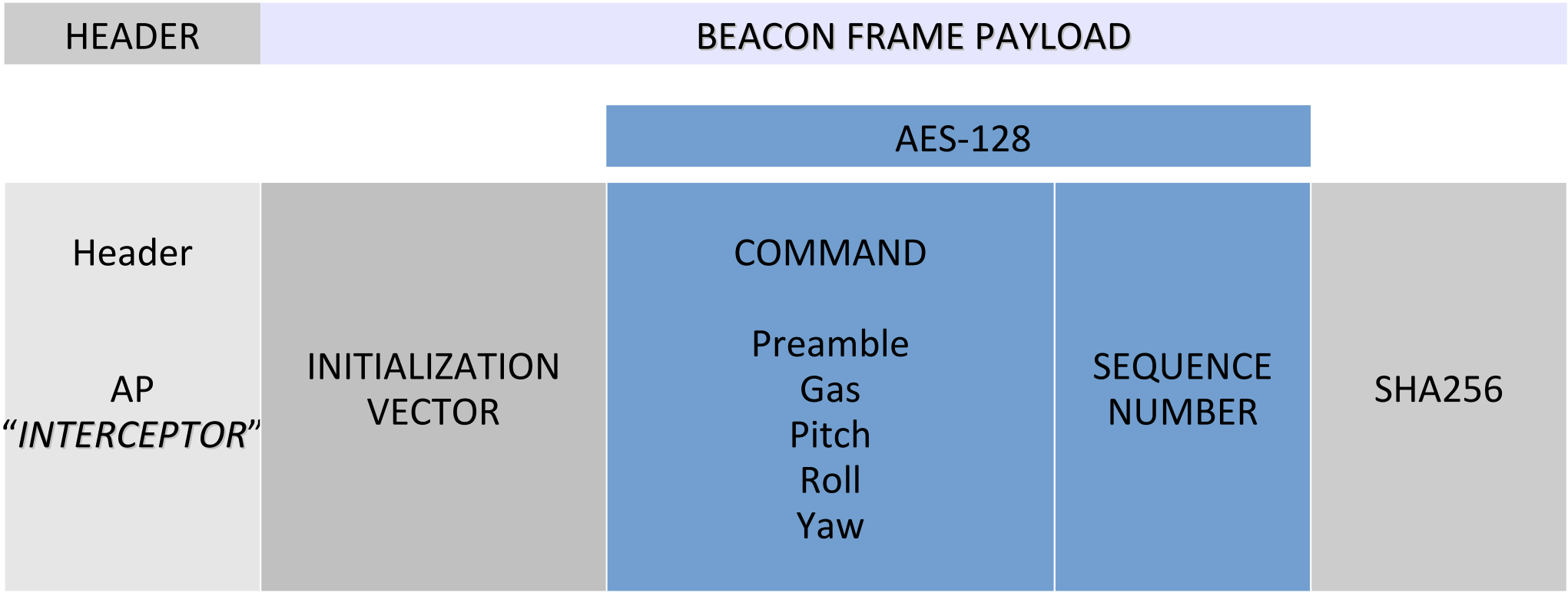
@taiksontexas

Interceptor WiFi architecture



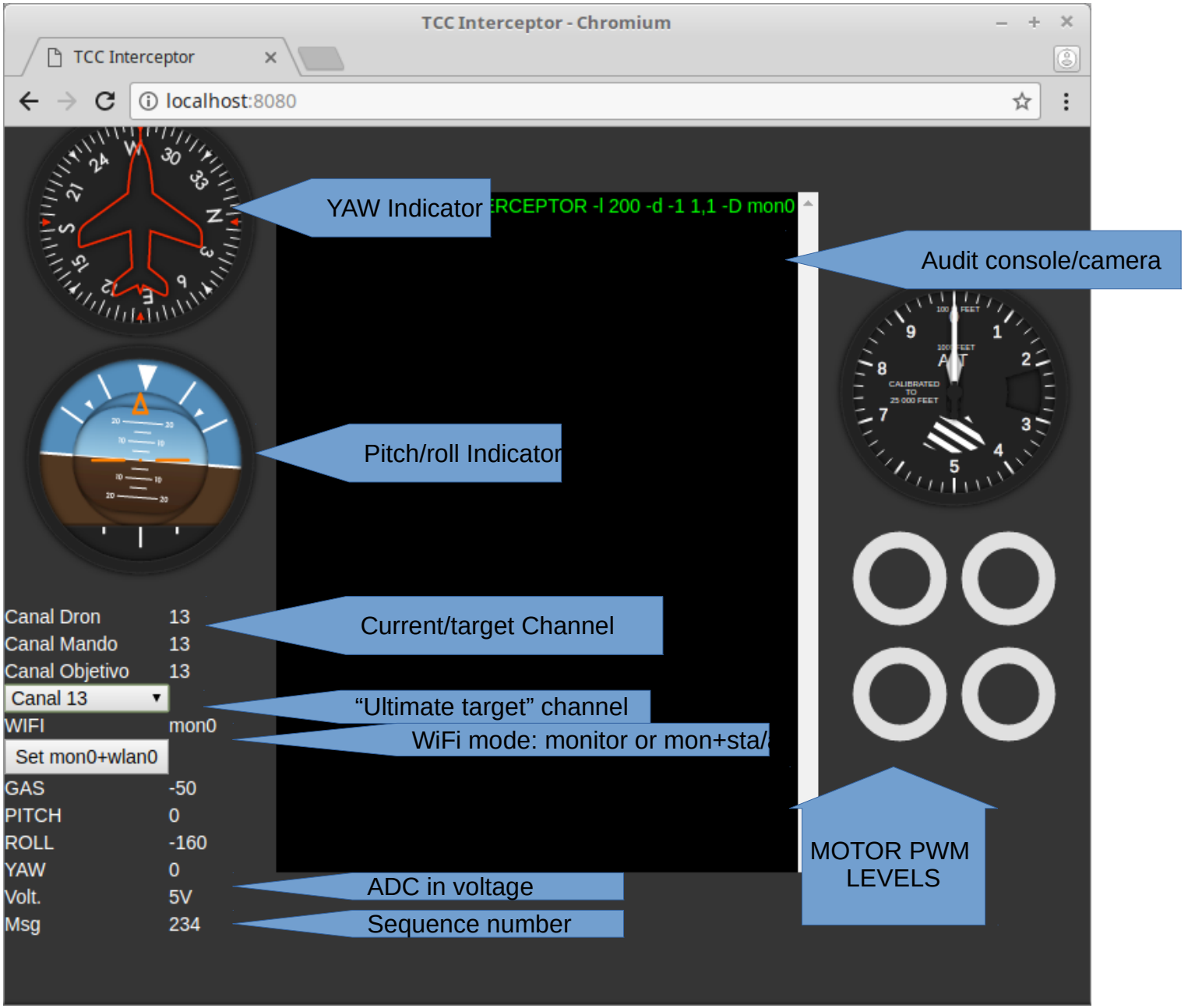
Interceptor WiFi architecture

Forged *Beacon Frame injection (PILOT SIDE)*



Interceptor WiFi architecture



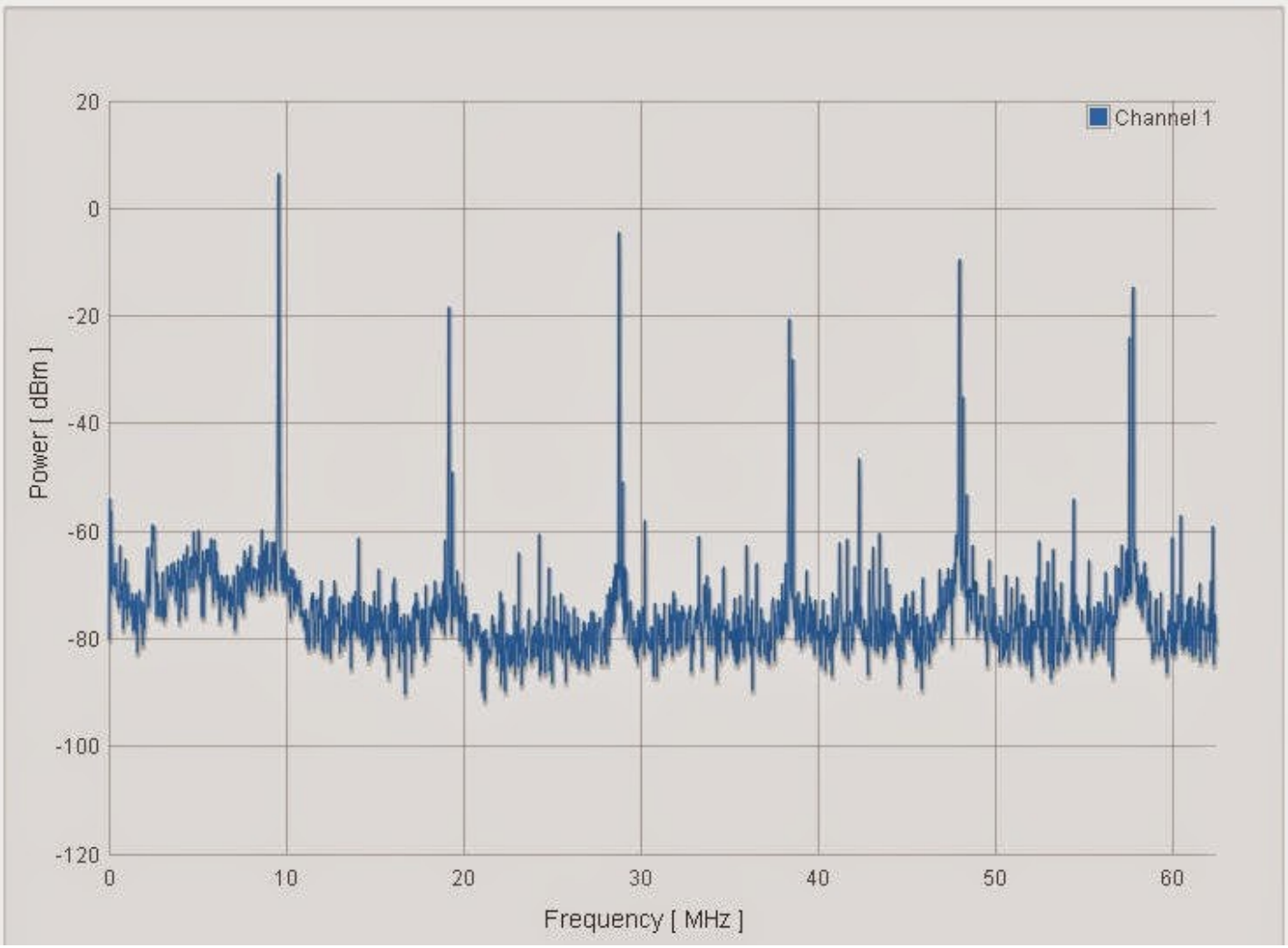


@taiksontexas

Fallback FM based TX

- For a WiFi complete jamming scenario
- Transmit with an arbitrary frequency
- Demo in FM band
- Transmitting in illegal frequencies are the least problem for bad guys
- Rpi radio transmission causes harmonics. Really a problem?

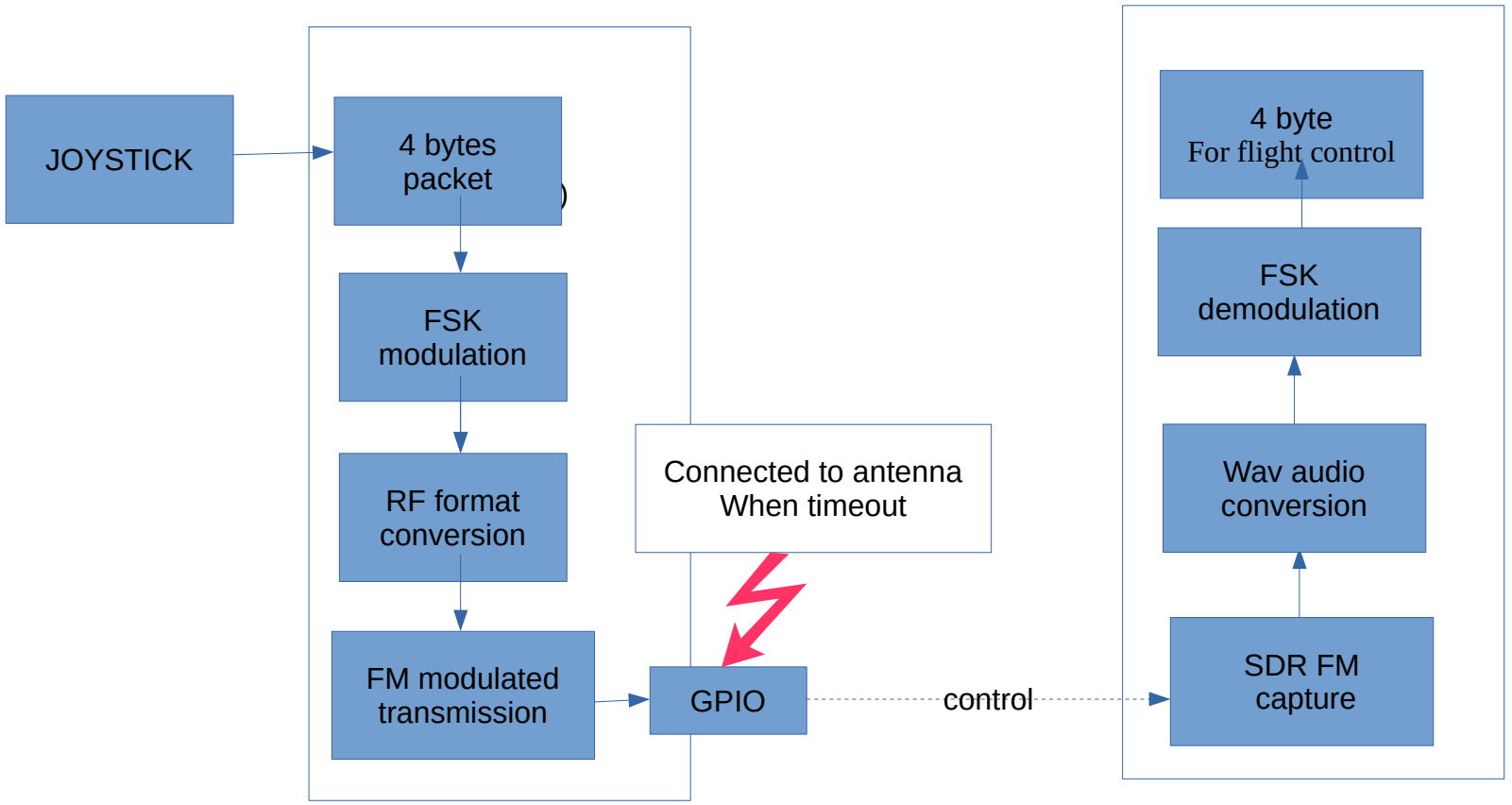
Fallback FM based TX



http://asliceofraspberrypi.blogspot.com/2014/10/generating-radio-frequencies-using.html

@taiksontexas

Fallback FM based TX




IT'S NO GOOD. I CAN'T MANEUVER!
STAY ON TOPIC!
made on imgur

Thank you!

Acknowledges:

José Manuel Hernández

Jesús Fernández

Javier Hernández

Vicente Polo

Daniel Iglesias

Adrian Aznar

David Meléndez Cano

R&D Embedded Systems Developer



@taiksontexas

Taiksonprojects.blogspot.com