Project “The Interceptor”:

Owning anti-drone systems with nanodrones

David Meléndez Cano
R&D Embedded Systems Developer

@taiksontexas

David Meléndez Cano

@TaiksonTexas

I+D Software Sistemas Embebidos

Autor Dron "Atropos" y ROV "Texas Ranger"

Autor del libro "Hacking con Drones"

Ed. 0xWord

blackhat

DEFCON

Campus Party™

SH3LLCON Security Hell Conference

ARDUINO DAY 2015

Madrid Mini Maker Faire

MORTERUELO CON

Albahaca Con

ISACA

8.8

LOCARD

HACK & BEERS

HONG KONG OPEN SOURCE CONFERENCE

CYBER CAMP 2014

NAVAJA NEGRA CONFERENCE

SEC/ADMIN CONFERENCE

/Rooted

HACKRON

{codemotion}

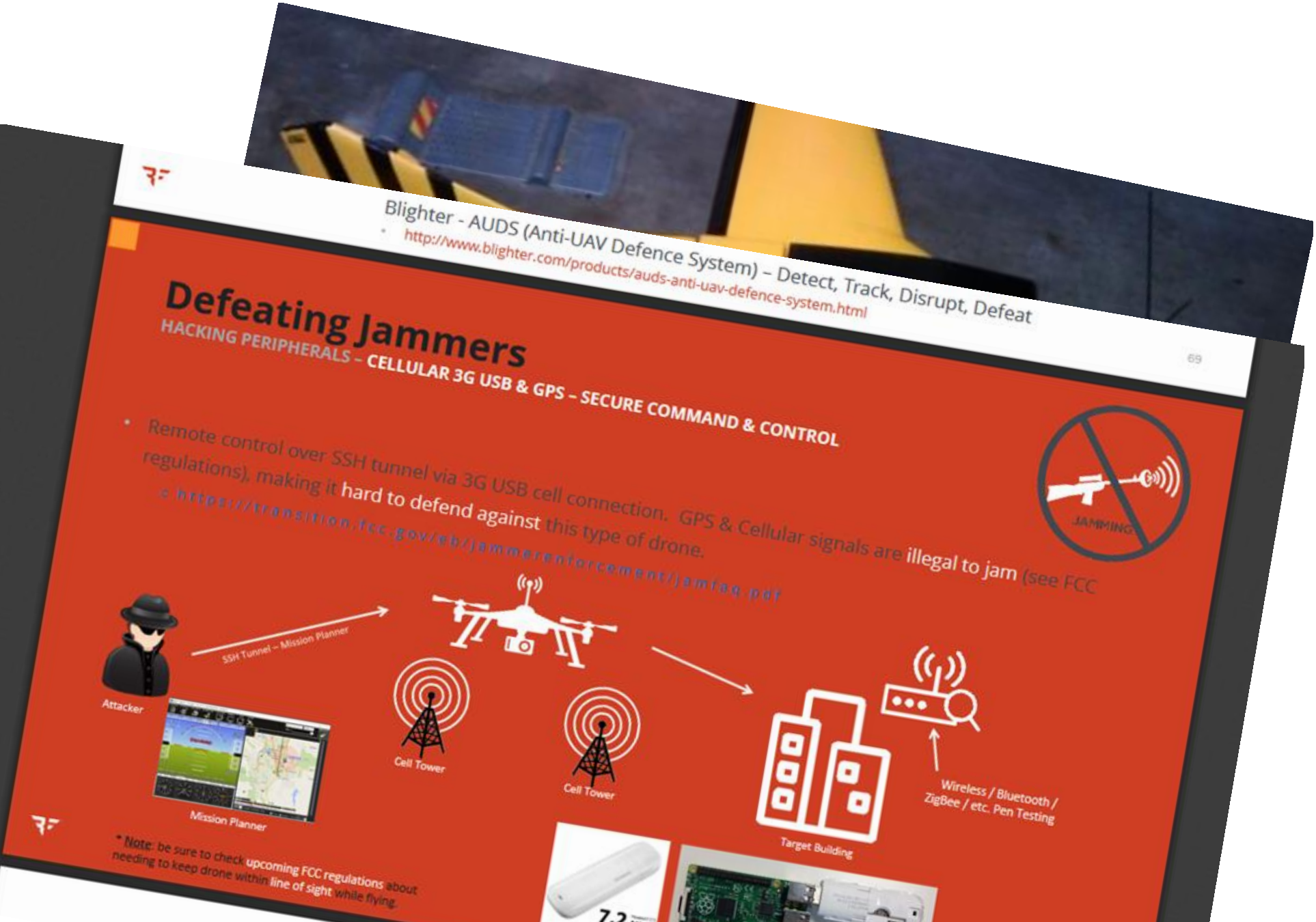
US & WORLD \ TECH \ NATIONAL SECURITY

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

Previously in DEFCON...

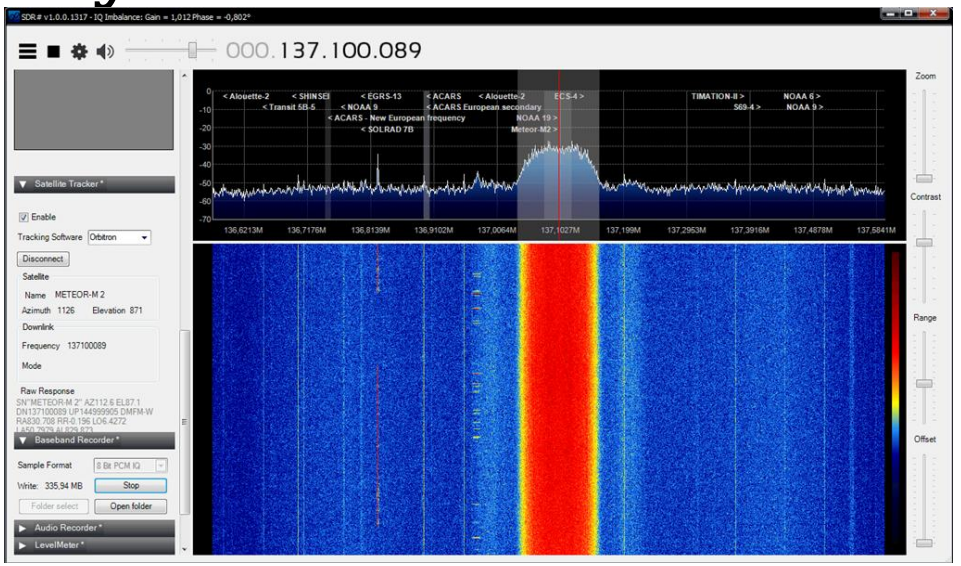


Drones as a threat

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

Detection

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

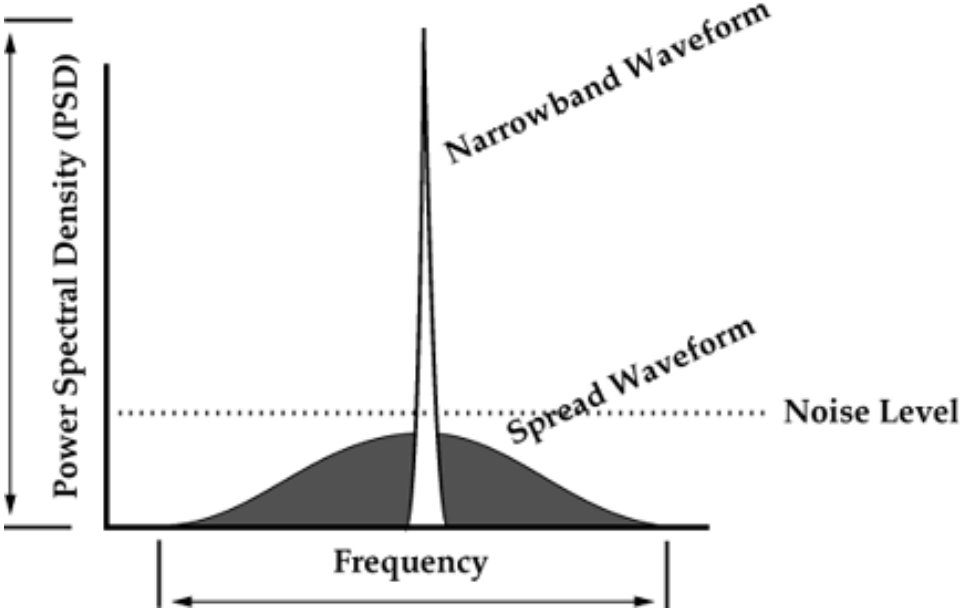


“Voluntary” measures

- 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 all “*everything will be alright*”

Counter-Countermeasures

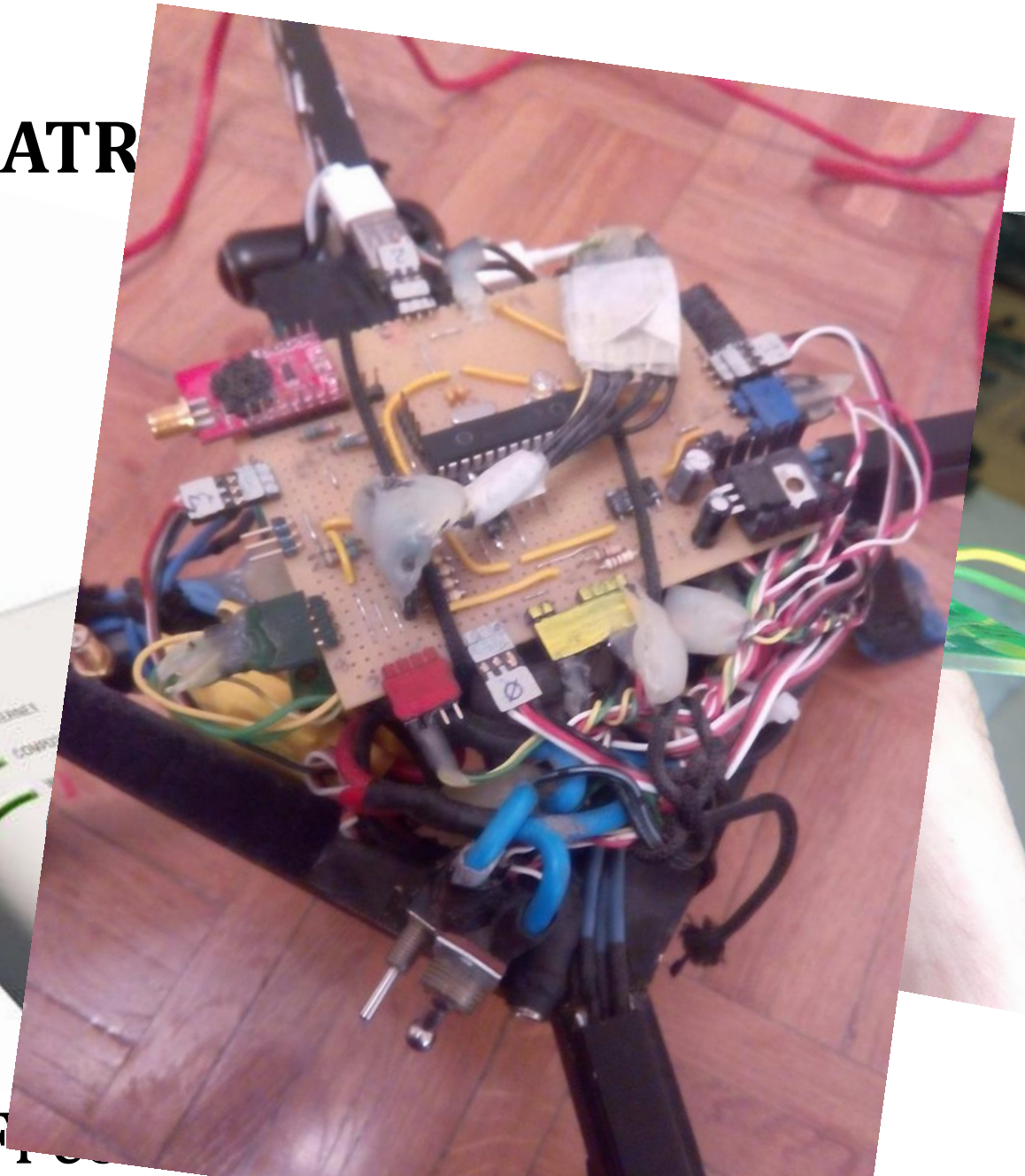
- Spread-spectrum
- Frequency hopping
- Use unespected frequencies by the jammer
- Robust protocols

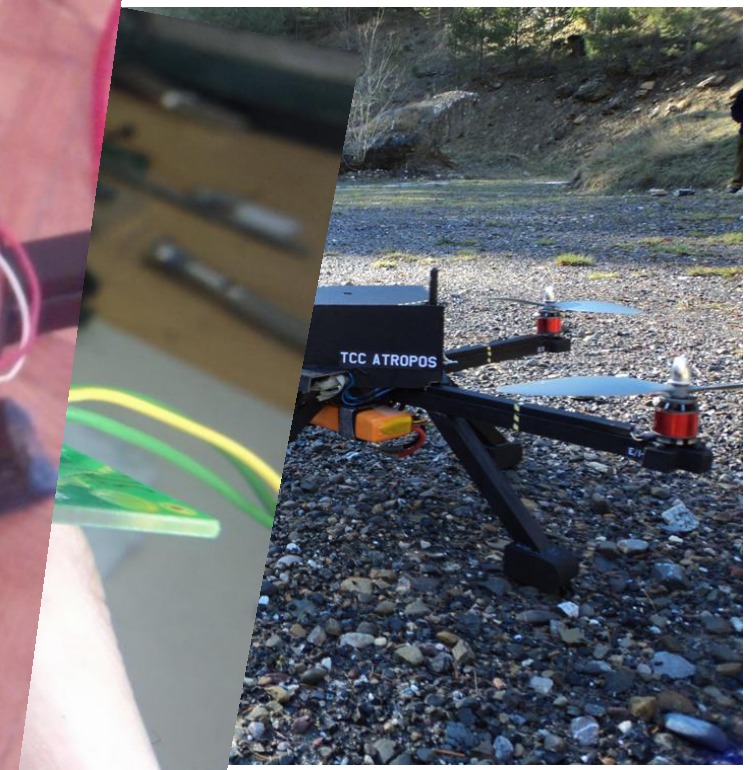


First Round: "**ATROPOS**"

Dron **ATR**

-
-





- WiF

Now, what else?

"We count thirty Rebel ships, Lord Vader...

...but they're so small they're evading our tu

Proyect "***The Interceptor***"

Proyecto "*Interceptor*"

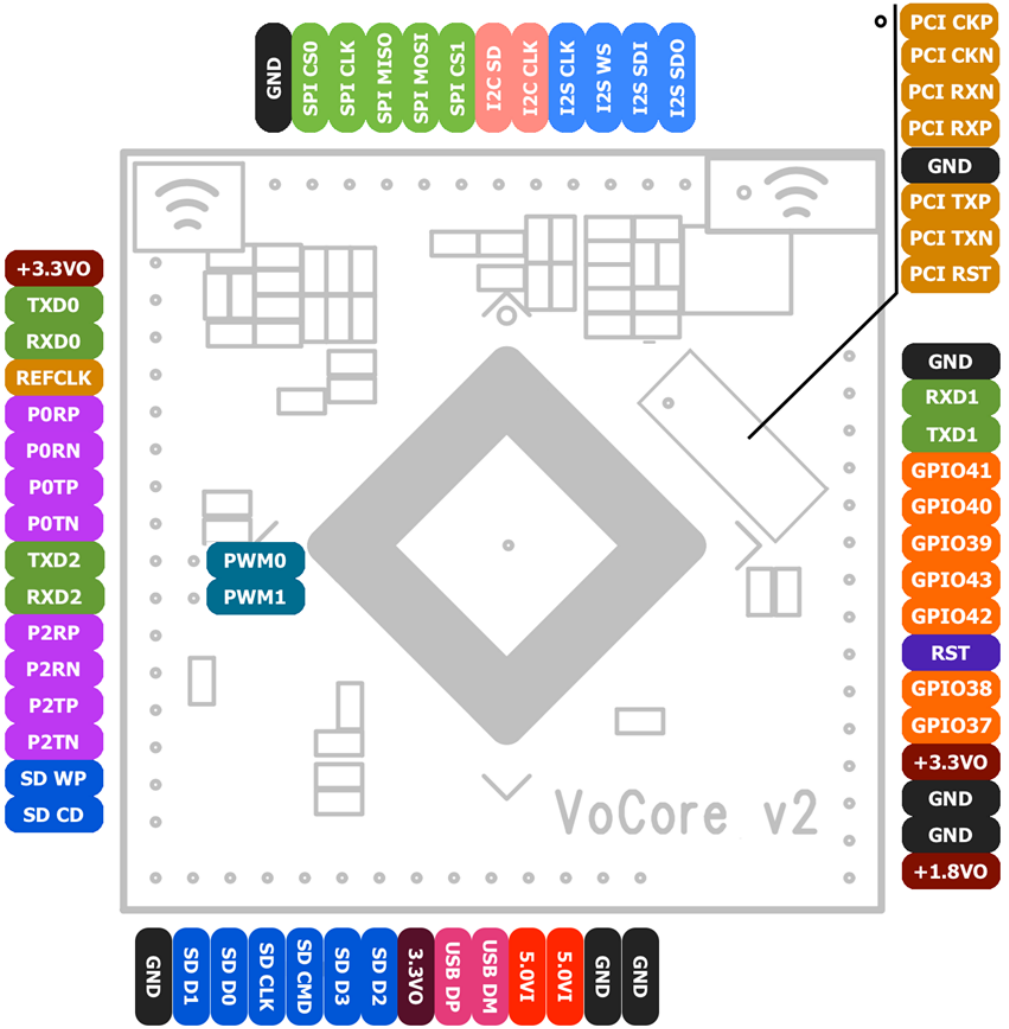
- Minimum size and weight (harder to detect)

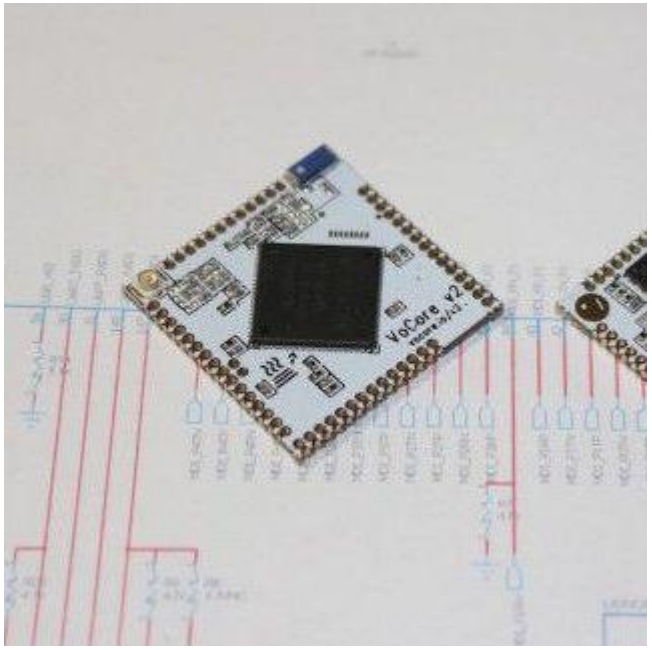
- Low budget *(no, seriously, really low)*

  ~$40 + $20 with SDR

- Hacking capabilities
- "Resilient" control

Vocore2


GND
SPI CS0
SPI CLK
SPI MISO
SPI MOSI
SPI CS1
I2C SD
I2C CLK
I2S CLK
I2S WS
I2S SDI
I2S SDO
PCI CKP
PCI CKN
PCI RXN
PCI RXP
GND
PCI TXP
PCI TXN
PCI RST
+3.3VO
TXD0
RXD0
REFCLK
P0RP
P0RN
P0TP
P0TN
TXD2
RXD2
P2RP
P2RN
P2TP
P2TN
SD WP
SD CD
PWM0
PWM1
GND
RXD1
TXD1
GPIO41
GPIO40
GPIO39
GPIO43
GPIO42
RST
GPIO38
GPIO37
+3.3VO
GND
GND
+1.8VO
VoCore v2
GND
SD D1
SD D0
SD CLK
SD CMD
SD D3
SD D2
3.3VO
USB DP
USB DM
5.0VI
5.0VI
GND
GND


VoCore v2

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.

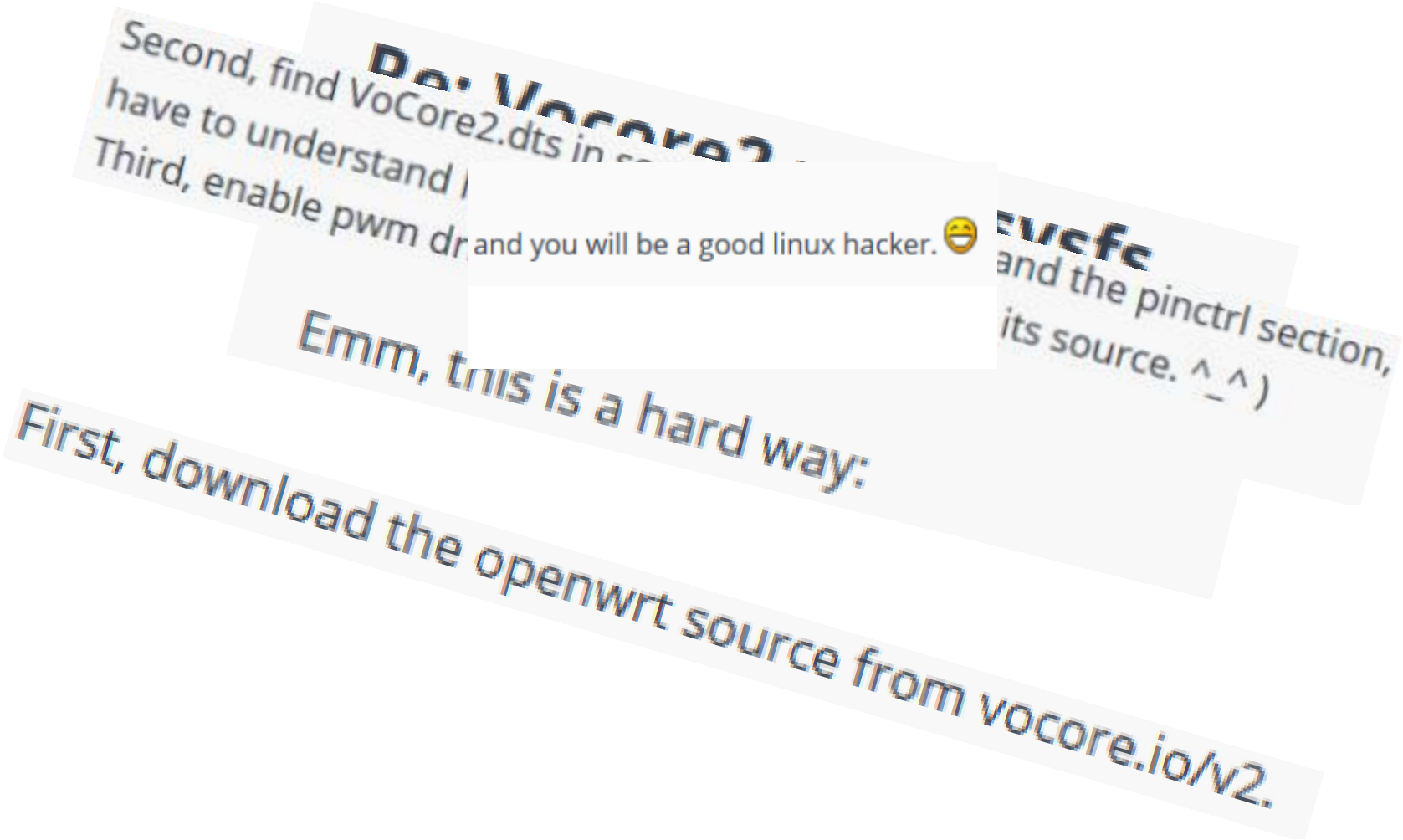
Vocore2

- Llega soporte para LEDE, ahora reunificado en OpenWRT
- DeviceTree completo y rediseñado
- Paso del mpu9250.
- Opciones: bno055, gy953 y sucedáneos

Vocore2: PWM

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

Vocore2: PWM in the forum



Vocore2: pinmux mt7628

```
static struct rt2880_pmx_func pwm1_grp_mt7628[] = {
    FUNC("sdxc d6", 3, 19, 1),
    FUNC("utif", 2, 19, 1),
    FUNC("gpio", 1, 19, 1),
    FUNC("pwm1", 0, 19, 1),
};

static struct rt2880_pmx_func pwm0_grp_mt7628[] = {
    FUNC("sdxc d7", 3, 18, 1),
    FUNC("utif", 2, 18, 1),
    FUNC("gpio", 1, 18, 1),
    FUNC("pwm0", 0, 18, 1),
};

static struct rt2880_pmx_func uart2_grp_mt7628[] = {
    FUNC("sdxc d5 d4", 3, 20, 2),
    FUNC("pwm", 2, 20, 2),
    FUNC("gpio", 1, 20, 2),
    FUNC("uart2", 0, 20, 2),
};
```

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

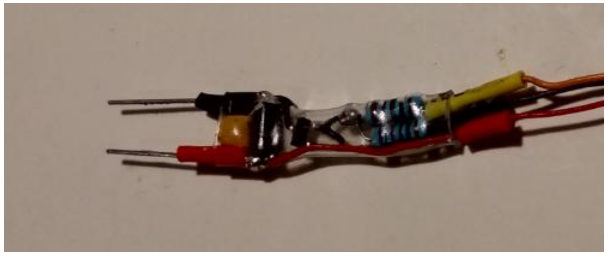
3.3.20 PWM_CH1 pin share scheme

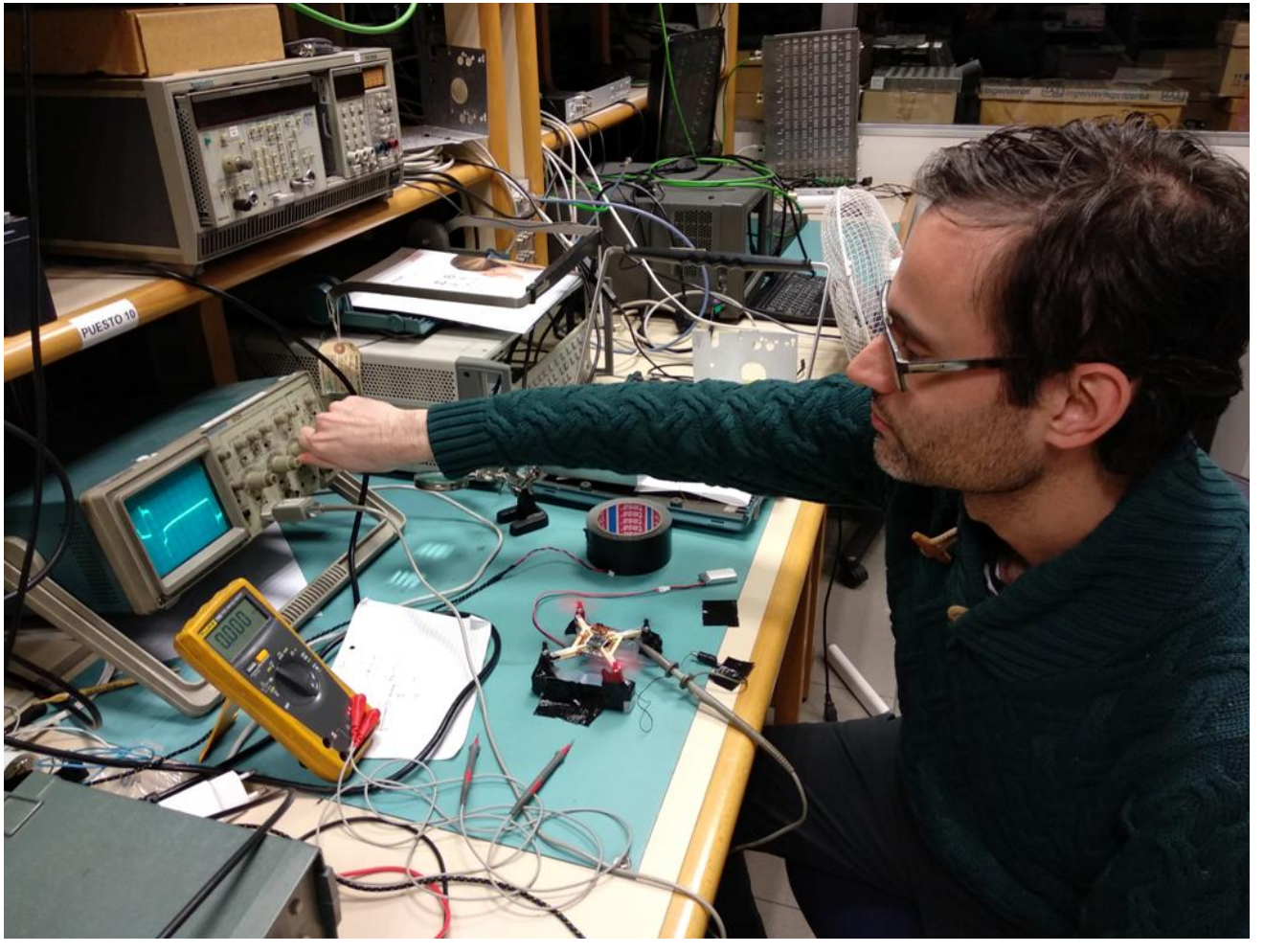
Controlled by the EPHY_APGIO_AIO_EN[4:1] and PWM1_MODE registers

	4'b0000	4'b1111

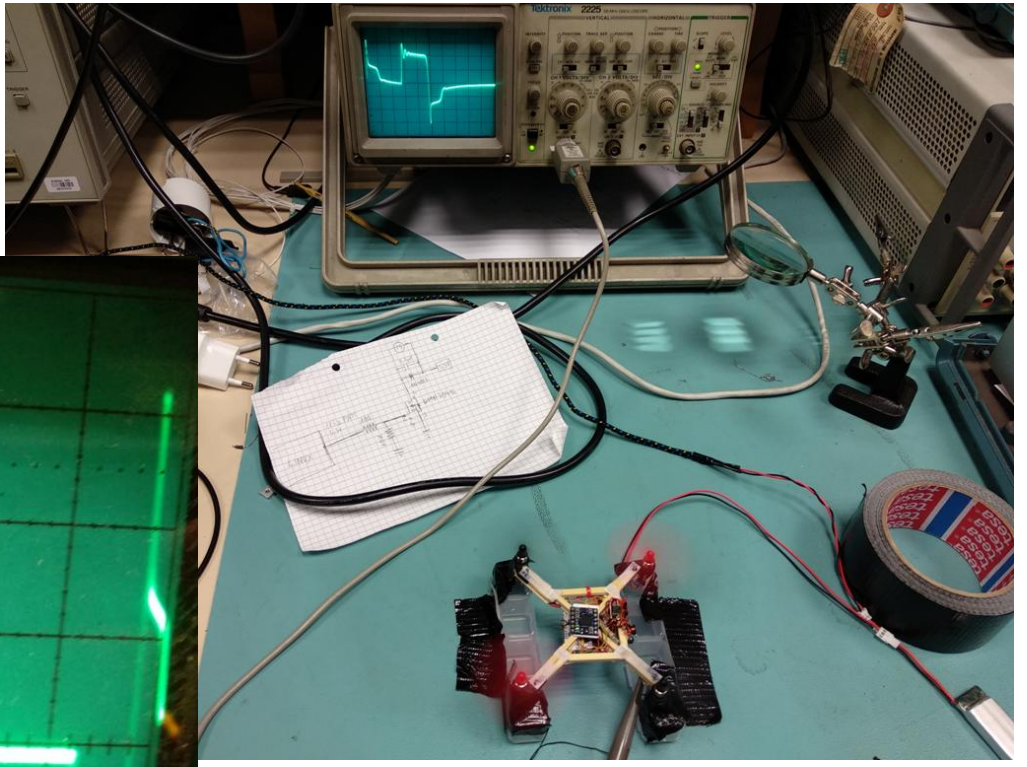
Power stage

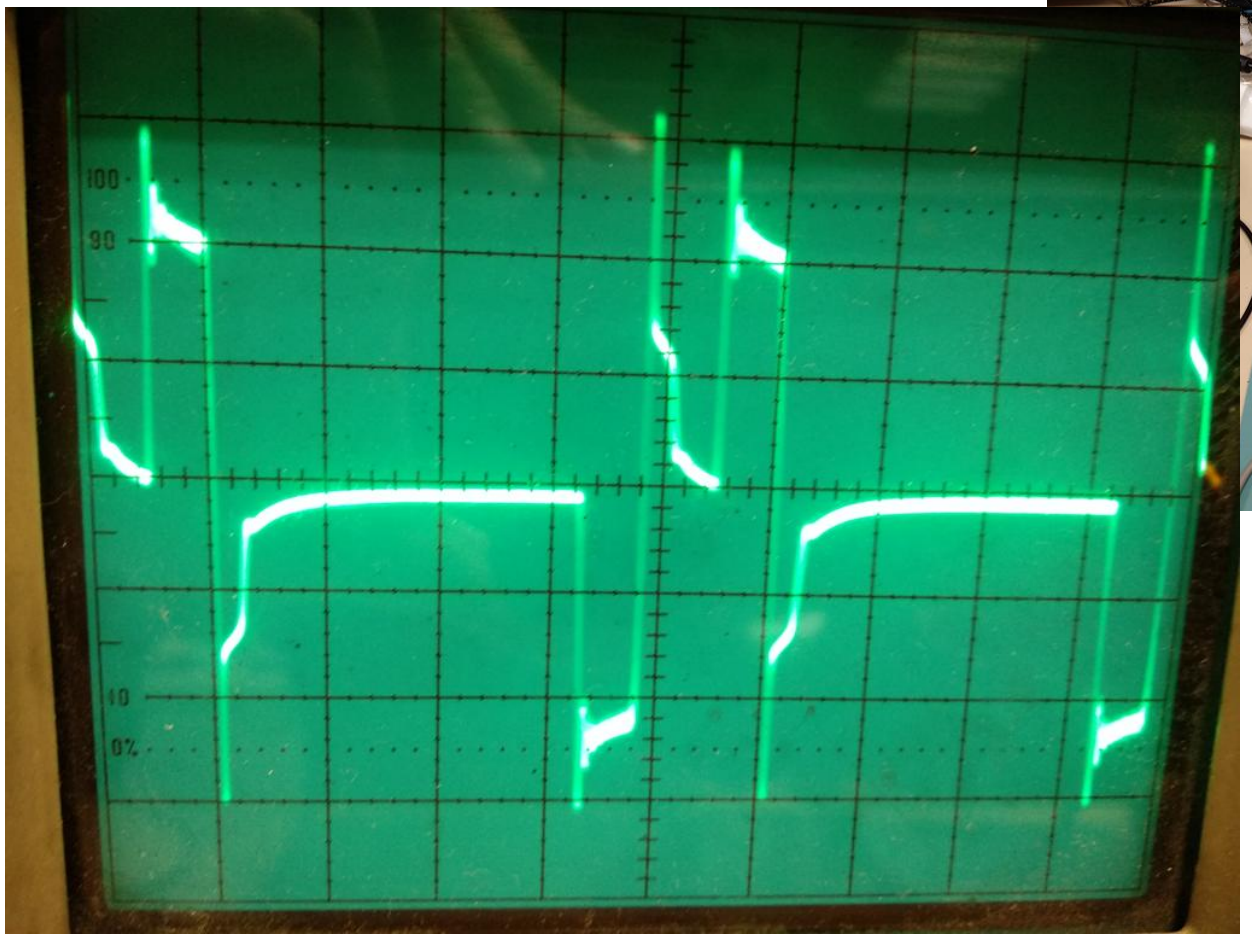
- Brushed motors (cheap as hell)
- X1 MOSFET
- X1 Capacitor
- X1 Schottky
- diode



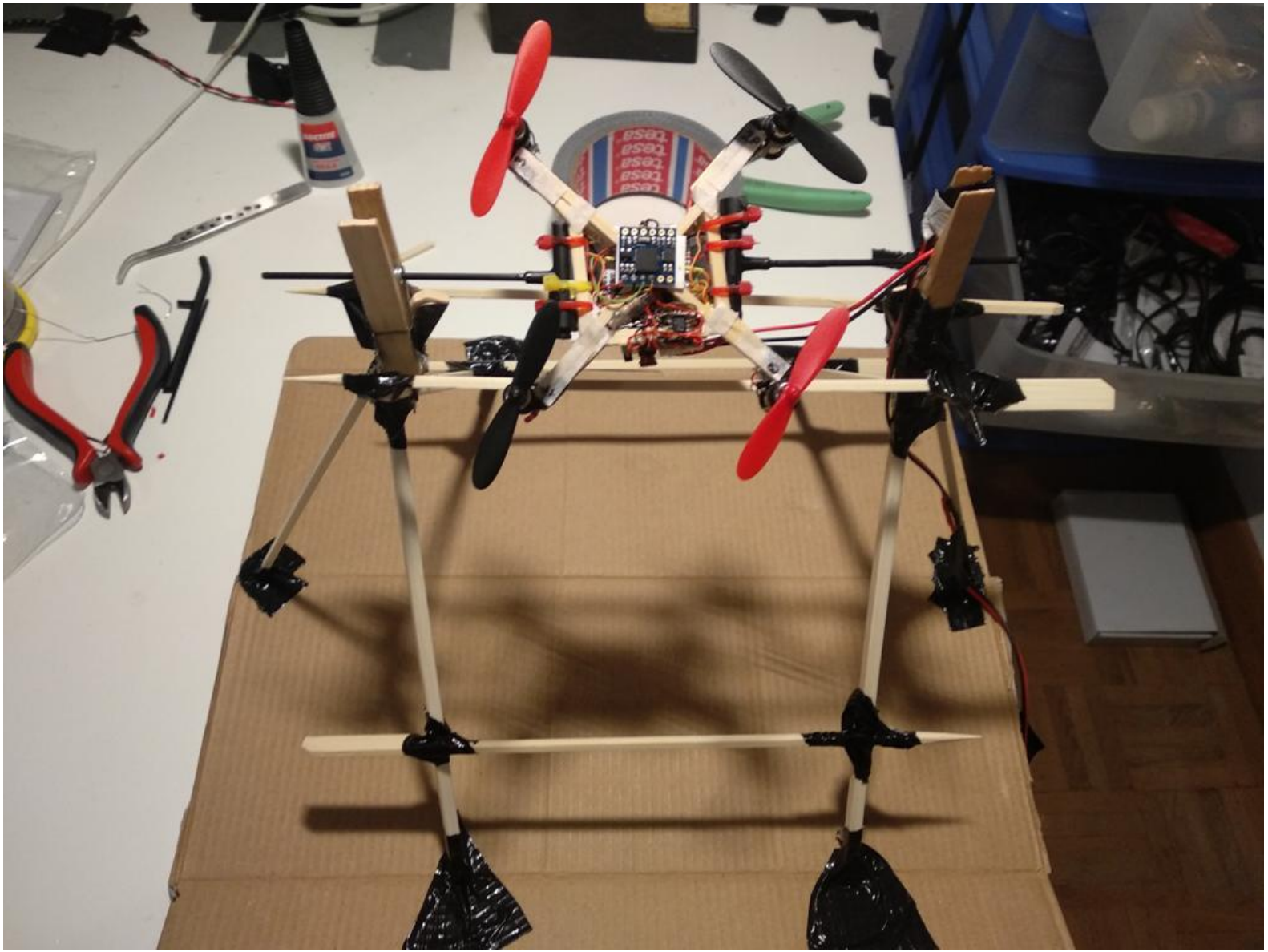


Electrical motor behaviour





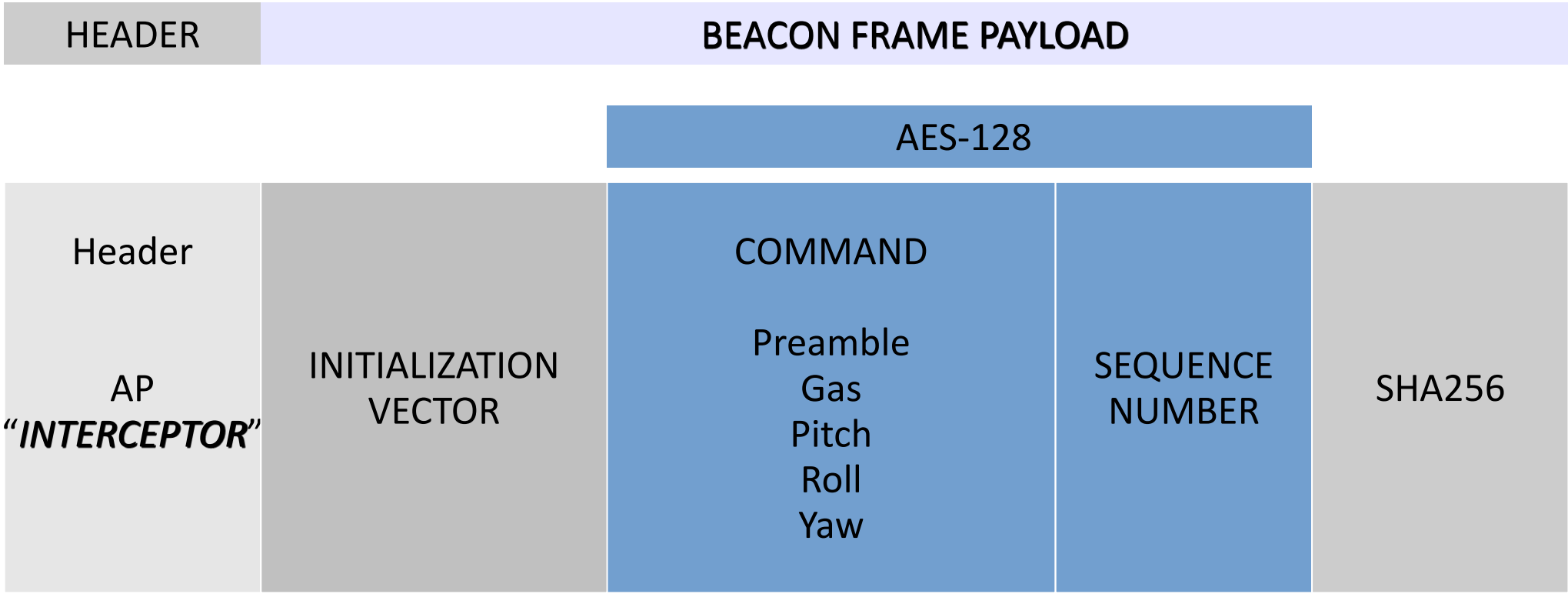
PID tunning



Interceptor como herramienta de hacking

- Control y telemetría por WIFI
- Protocolo RX/TX beacon Frames
- Herramientas de hacking WiFi en Vocore2
- Salto de canales sin interrupción
- Sólo se usa una interfaz WiFi en el dron
- Cifrado AES-CBC
- Hash SHA256

Forged *Beacon Frame injection (PILOT SIDE)*



SDR con chip de FESCO?

¿Preguntas?

Agradecimientos:

José Manuel Hernández

Jesús Fernández

Javier Hernández

Vicente Polo

David Meléndez Cano

R&D Embedded Systems Developer

@taiksontexas