Strategies to Harden and Neutralize UAVs using RF DEW

José Lopes Esteves,

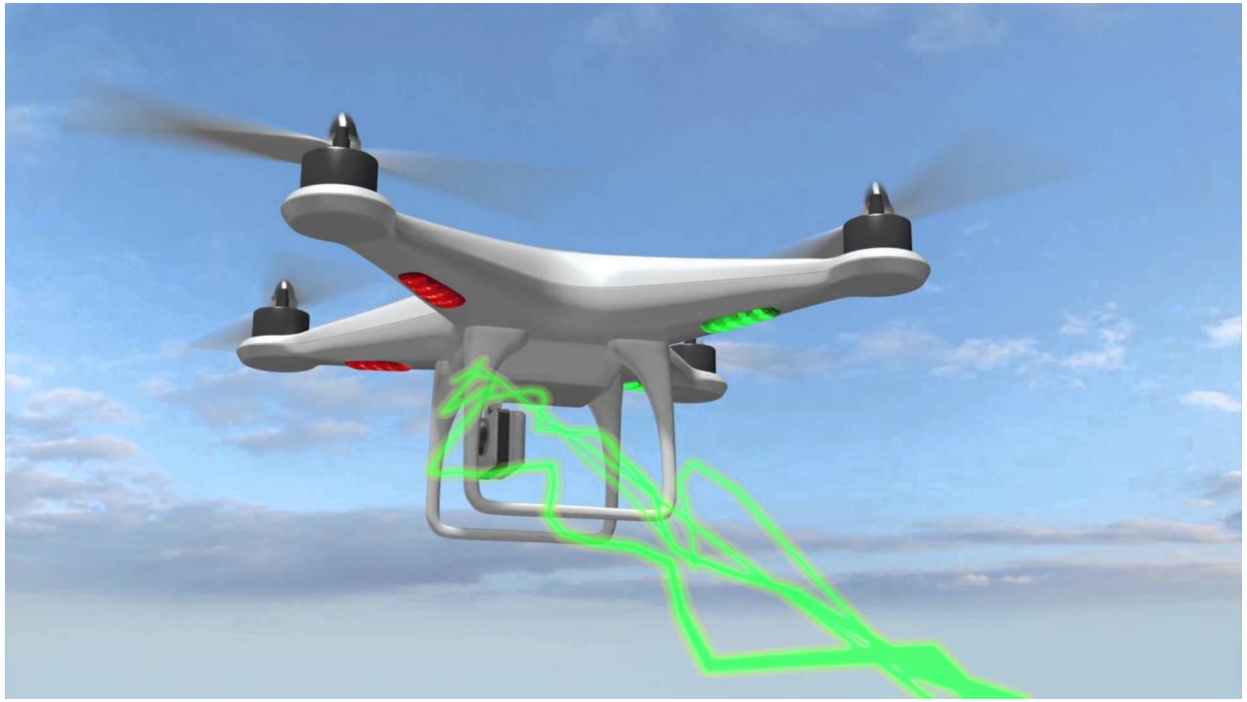
Emmanuel Cottais and Chaouki Kasmi

ABOUT THE AUTHORS

- ANSSI: National Cybersecurity Agency of France
- Wireless Security Lab
  - 10 members, 2 PhDs, 2 PhD students
  - Electromagnetic Security (TEMPEST, IEMI)
  - Wireless Communications Security (mobile communication, Wi-Fi, Bluetooth, RFID, etc.)
  - Embedded Systems
  - Physical layer
  - Signal Processing

AGENDA

- Context
- UAV Neutralization
- RF DEW
- Instrumentation journey
- Effects observation
- Conclusion



Context

Civilian Unmanned Aerial Vehicles

CONTEXT

- UAVs are spreading fast
  - Civilian drones getting cheaper and efficient
  - Used in critical operations

JEREMY HSU SECURITY 01.23.17 07:07 AM

THE MILITARY MAY SOON BUY THE SAME DRONES YOU DO

La préfecture de police de Paris forme ses télépilotes

22 janvier 2016

Air Platforms

IDF buying mass-market DJI drones

Yaakov Lappin, Tel Aviv and Jeremy Binnie, London - Jane's Defence Weekly

15 June 2017

Minidrones et nanodrones : allier innovation et flexibilité

Continuer à développer ou à acquérir des **produits militaires innovants**

Mais ne pas s'interdire d'acquérir des **drones commerciaux**, qui peuvent également se révéler utiles à très faible coût

US – DoD pulls the plug on COTS drones

By Gary Mortimer - 7 June 2018

CONTEXT

- UAVs are spreading fast
  - Civilian drones getting cheaper and efficient
  - Used in critical operations
  - And potentially for malicious uses

Enquête ouverte après le survol par un drone du fort de Brégançon où séjourne Emmanuel Macron

Selon le parquet de Toulon, l'engin a été neutralisé grâce à un brouillage d'ondes.

A Closer Look at the Drone Attack on Maduro in Venezuela

CONTEXT

- UAVs are spreading fast
  - Civilian drones getting cheaper and efficient
  - Used in critical operations
  - And potentially for malicious uses

- UAVs neutralization is needed
  - Several strategies
  - No perfect answer
  - RF DEW also considered [1]

UAV Neutralization

An introduction

UAVS NEUTRALIZATION

- Complex process
  - Detection
  - Identification
  - Neutralization
- Each step is a technical challenge
  - No ideal solution
  - Context dependent
- Between each step there can be human delays
  - Legal issues
  - Efficiency impact

UAVS NEUTRALIZATION

- Detection, identification
  - RF communication (spectrum, protocol, AP)
  - Acoustic : propeller noise
  - Visual: video cameras, thermal, IR, laser
  - Radar, goniometry, trilateration
  - Human awareness
  - Machine learning for classification (e.g. uav vs bird, P3 vs Bebop)

- Key points: distance, tracking, pilot location, accuracy, cost

UAVS NEUTRALIZATION

- Destruction
  - Ballistics, traditional weapons
  - **Directed Energy Weapons**

- Interception
  - Birds (e.g. hawks)
  - Net throwing guns
  - Interceptor drones (nets, ropes, parachutes)

UAVS NEUTRALIZATION

- Taking control
  - RF protocol weakness / RF stack vulnerability
  - Default credentials, misconfiguration
  - GPS spoofing

- Trigger special mode
  - RF communication jamming
  - GPS jamming

Radio Frequency Directed Energy Weapons

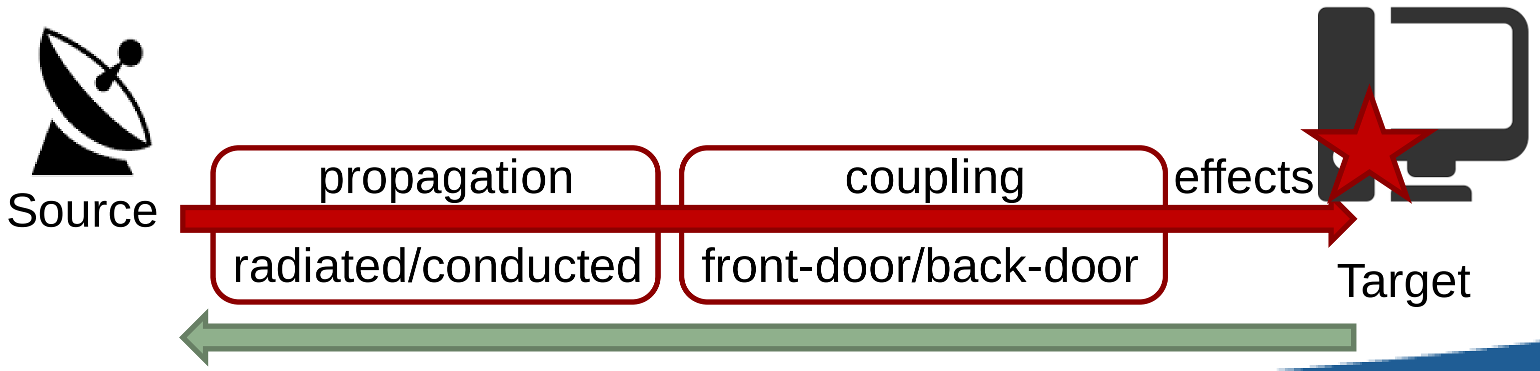
EM Susceptibility Assessment

RF DEW

- Electromagnetic weapons
  - Not only fantasy weapons in movies
  - Capabilities developed since 1990’s
    - HEMP – nuclear EM pulse
    - 10’s MHz to several GHz
    - RF directed energy weapons
  - Effects on electronic systems
    - Analysis of effects highly required
    - From HW to logical failure
    - Cascading effects
    - Appropriate protections

RF DEW

- Vulnerability testing and attack rating require
  - Source signal determination
  - Propagation chain estimation
  - Effects detection
  - Effects classification
  - Impact estimation



RF DEW

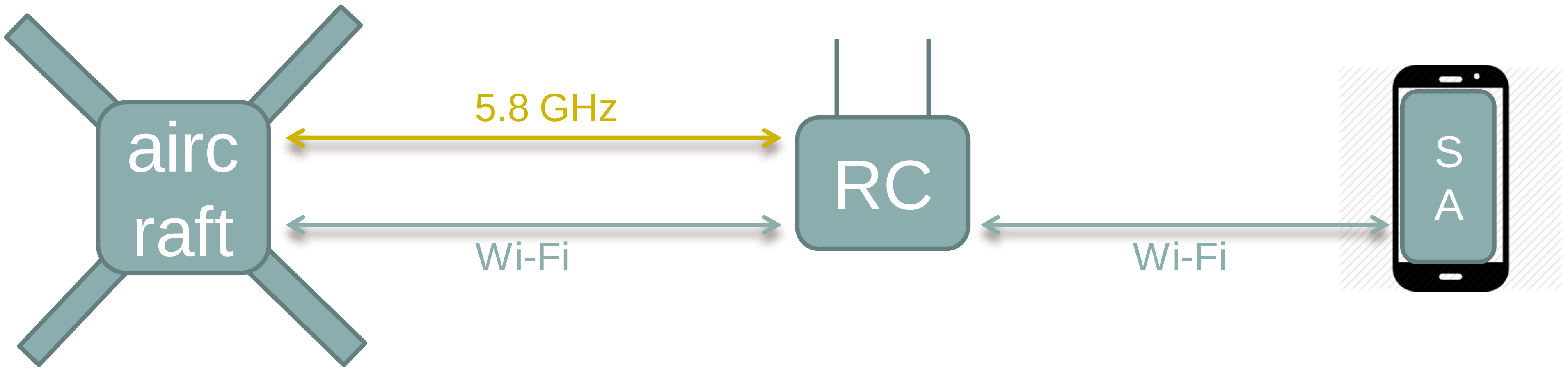
- Electromagnetic susceptibility assessment is necessary
  - For determining neutralization strategies
  - For proposing hardening solutions
- Previous work on UAVs [1-6]
  - Focus on RF front ends, self-jamming, interference from cellular networks
  - Motors malfunction
- Can our system centric approach [7] give more information ?
  - Which observables ?
  - How to run our software ?

Instrumentation journey

Making the target talk

INSTRUMENTATION JOURNEY

- The target



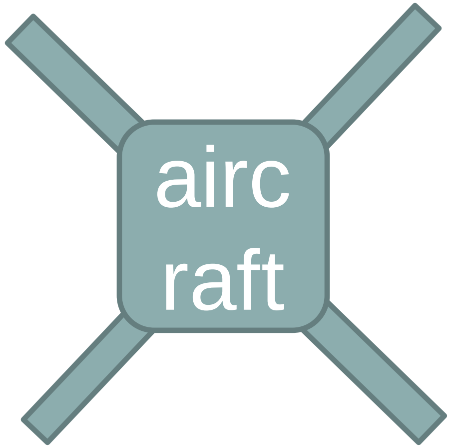
- Autopilot
  - Sensors (IMU)
  - Motors
  - Coordinating SoC
- GPS receiver
- Wi-Fi client
- 5.8GHz Radio

- Wi-Fi access point
- 5.8GHz Radio
- Control commands

- Wi-Fi client
- User interface
  - Telemetry
  - Configuration

INSTRUMENTATION JOURNEY

➢ Observables



Coupling	Hardware Interfaces	Software observables
Front door	•GPS •Wi-Fi •5.8GHz Radio	•Signal quality •Communication rate •Link errors
Back door	•Autopilot •Sensors (IMU) •Motors •Coordinating SoCs	•Raw sensor readings •Inferred information •Motors state and feedback •Operating system state •Embedded communication interfaces state

INSTRUMENTATION JOURNEY

- Now how to
  - Run our own software
  - Access to observables

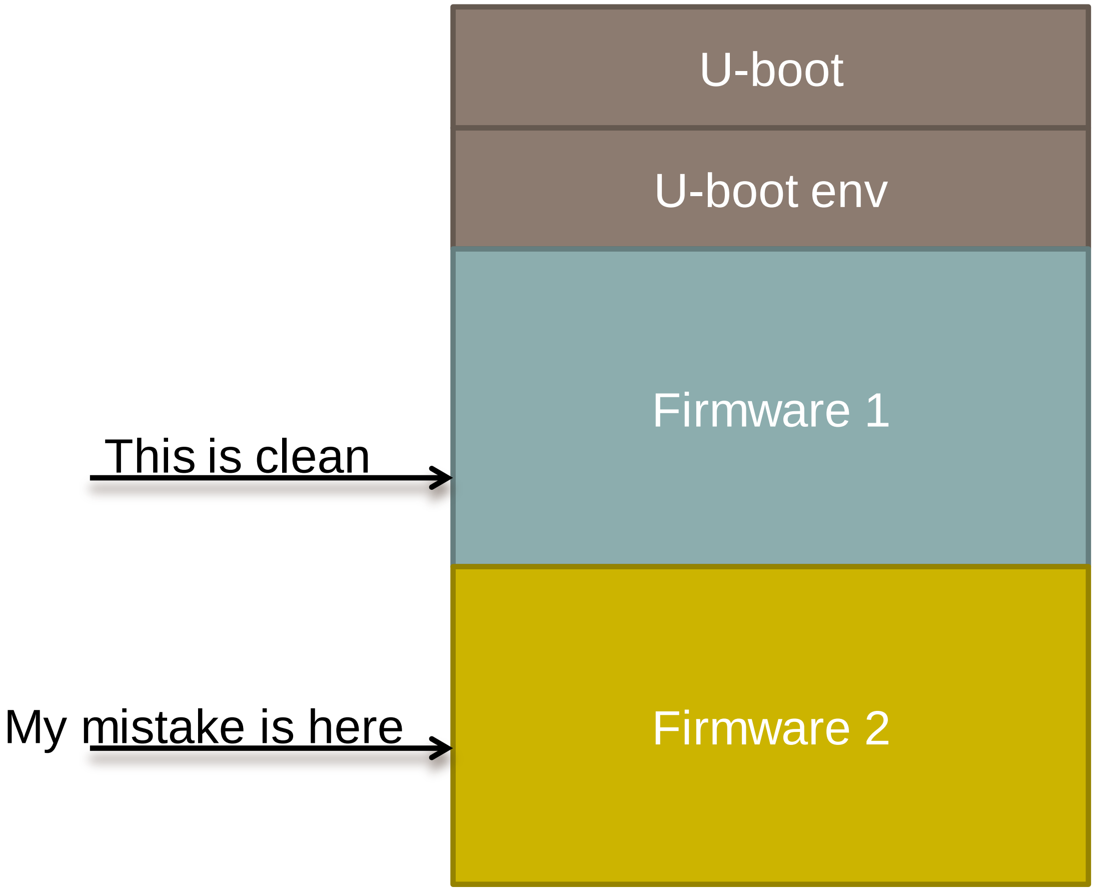
- Hardware and software analysis
  - Find a way to root
  - Find where observables are processed
  - Understand how they are processed
  - Design and deploy observation software
  - Route data to monitoring computer

INSTRUMENTATION JOURNEY

- Find a way to root
  - There is a documented weakness
  - Access to Wi-Fi with default PSK and enjoy a root telnet
- First system discovery (software)
  - Hardware architecture: Atheros MIPS
  - System: OpenWRT
  - Partitions, file system: squashFS /JFFS2 overlay
  - Wi-Fi config, vendor software
- Modification of startup sequence
  - Wi-Fi interface does not start anymore

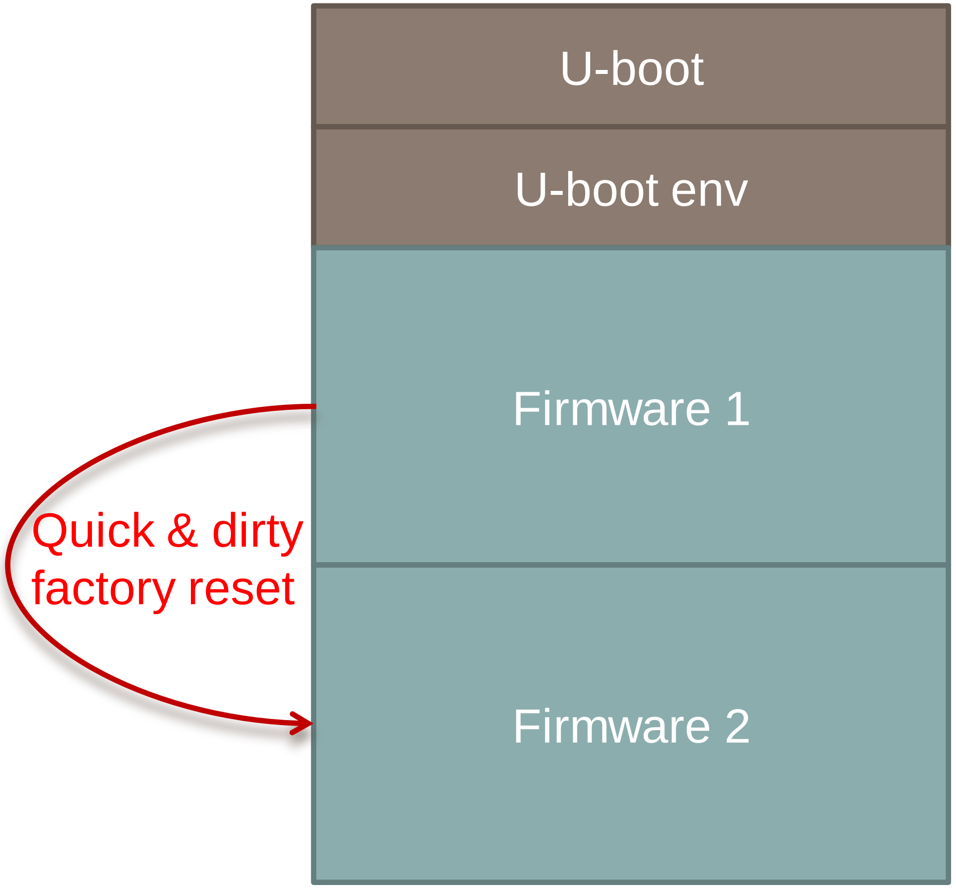
INSTRUMENTATION JOURNEY

- Find way back to root
  - Search ‘factory reset’: nope
  - Open the target
  - Locate the Atheros chip
  - The flash memories around
  - Sniff SPI on bootup to confirm
  - Unsolder, dump the flash



INSTRUMENTATION JOURNEY

- Find way back to root
  - Search 'factory reset': nope
  - Open the target
  - Locate the Atheros chip
  - The flash memories around (SPI NOR)
  - Sniff SPI on bootup to confirm
  - Unsolder, dump the flash
  - Reflash, reinsert and resolder



INSTRUMENTATION JOURNEY

- Find another way to root
  - But the box is open
  - Plenty of labelled test points
  - ‘UART’ or ‘URAT’ ☺, and also USB, I2C, SPI, PWM, PPM, SWD…

- Sniff on bootup
  - Uboot exposes a console
  - OpenWRT exposes a root shell
  - With a small busybox
  - And internet already knew it

INSTRUMENTATION JOURNEY

- Vendor software analysis
  - Listens on a serial port
  - Masks packets, sends them over Wi-Fi
  - A debug flag logs all cleartext packets to syslog

- Analyzing serial ports
  - Mostly same baud rate & frame structure
  - Several sensors, several SoCs
  - Maybe our observables?
  - How to decode and interpret ?

INSTRUMENTATION JOURNEY

- Mobile software analysis
  - Receives the data
  - Unmasks the packets
  - Parses some of them for GUI
  - Masks some of them in a flight log file

- What do we have ?
  - Motor states, battery info, aircraft attitude, sensor values (IMU), GPS data, RF link info, camera gimbal data
  - Everything from the GUI, plus some extras

INSTRUMENTATION JOURNEY

- Final strategy
  - Run the debug mode of vendor software
  - Configure syslog to remote IP
  - Run extra scripts and also log to syslog
  - Parse the packets, store and plot in real time on remote machine

- Ready for susceptibility testing

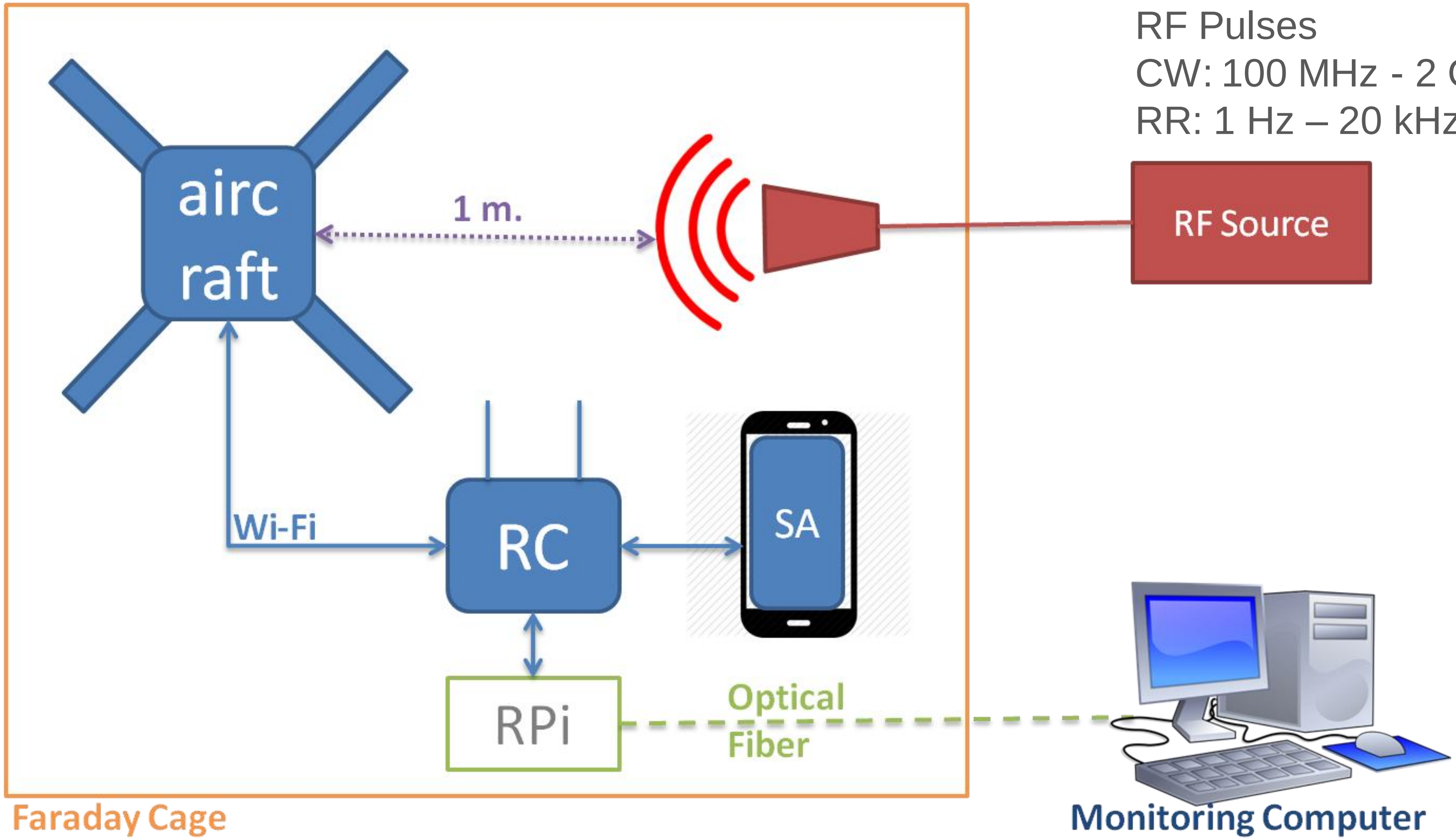
- Let’s go to the Faraday cage

Effects observation

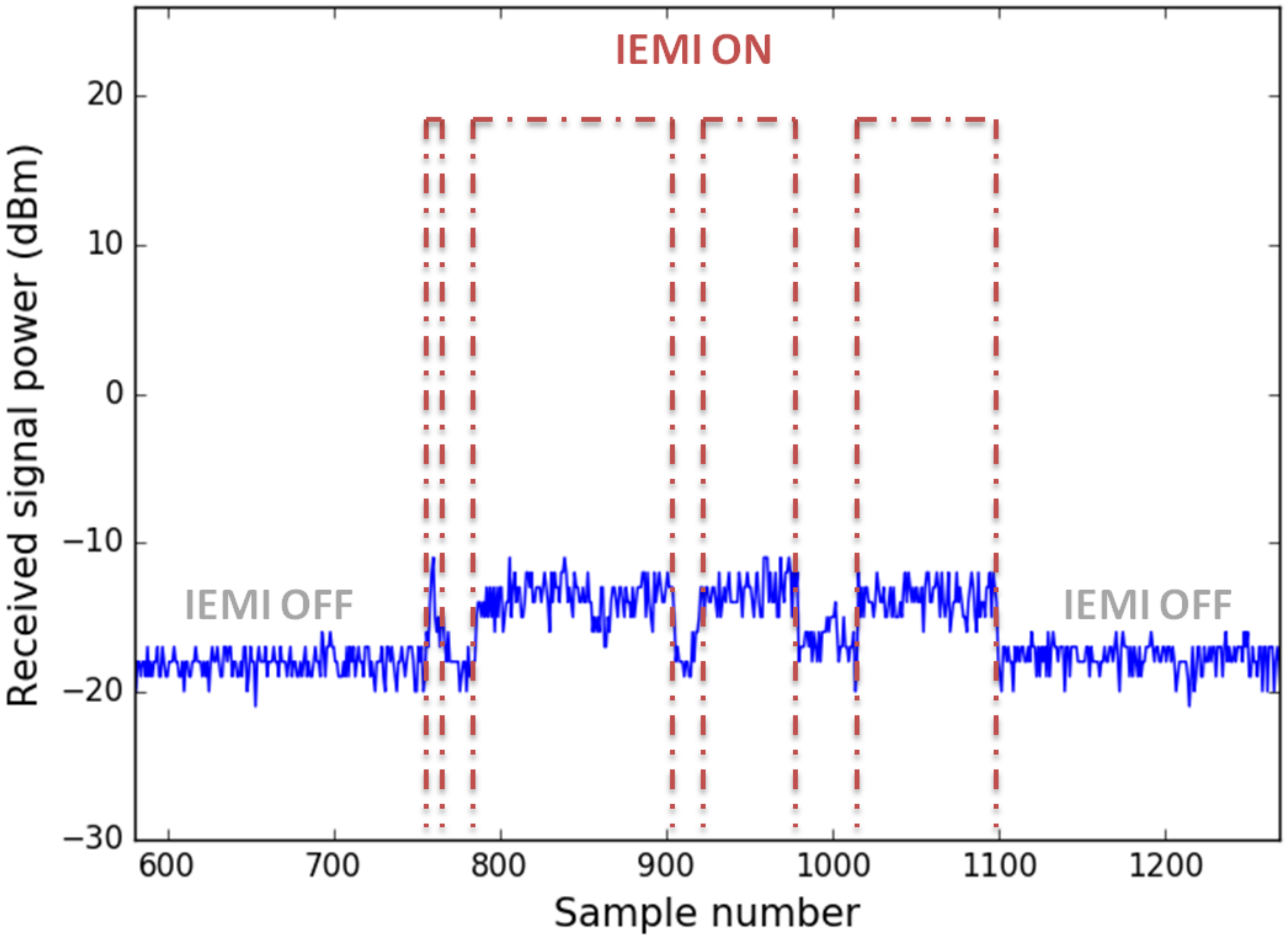
Further than disruption

EFFECTS: TEST SETUP

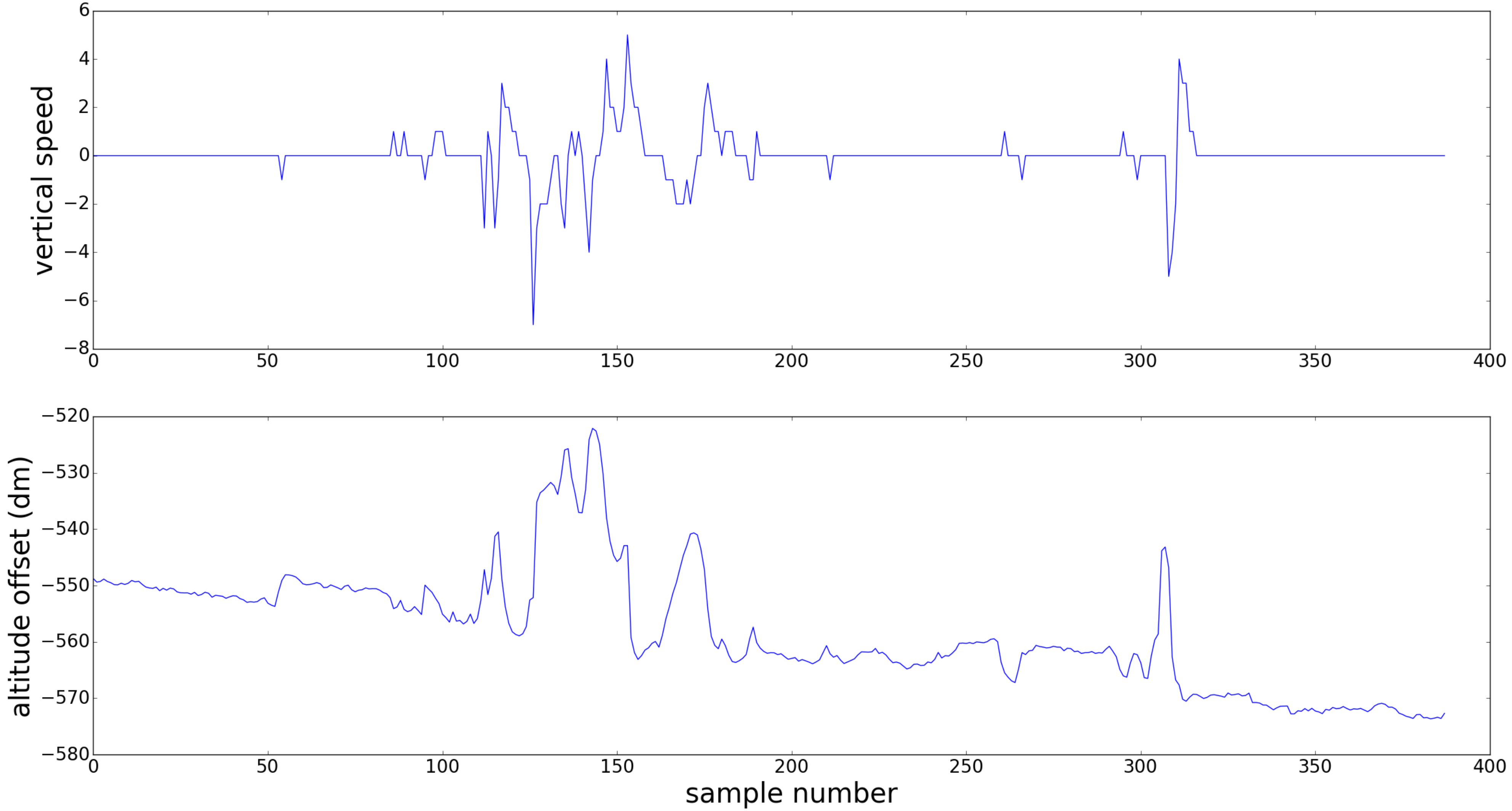
RF Pulses
CW: 100 MHz - 2 GHz
RR: 1 Hz – 20 kHz



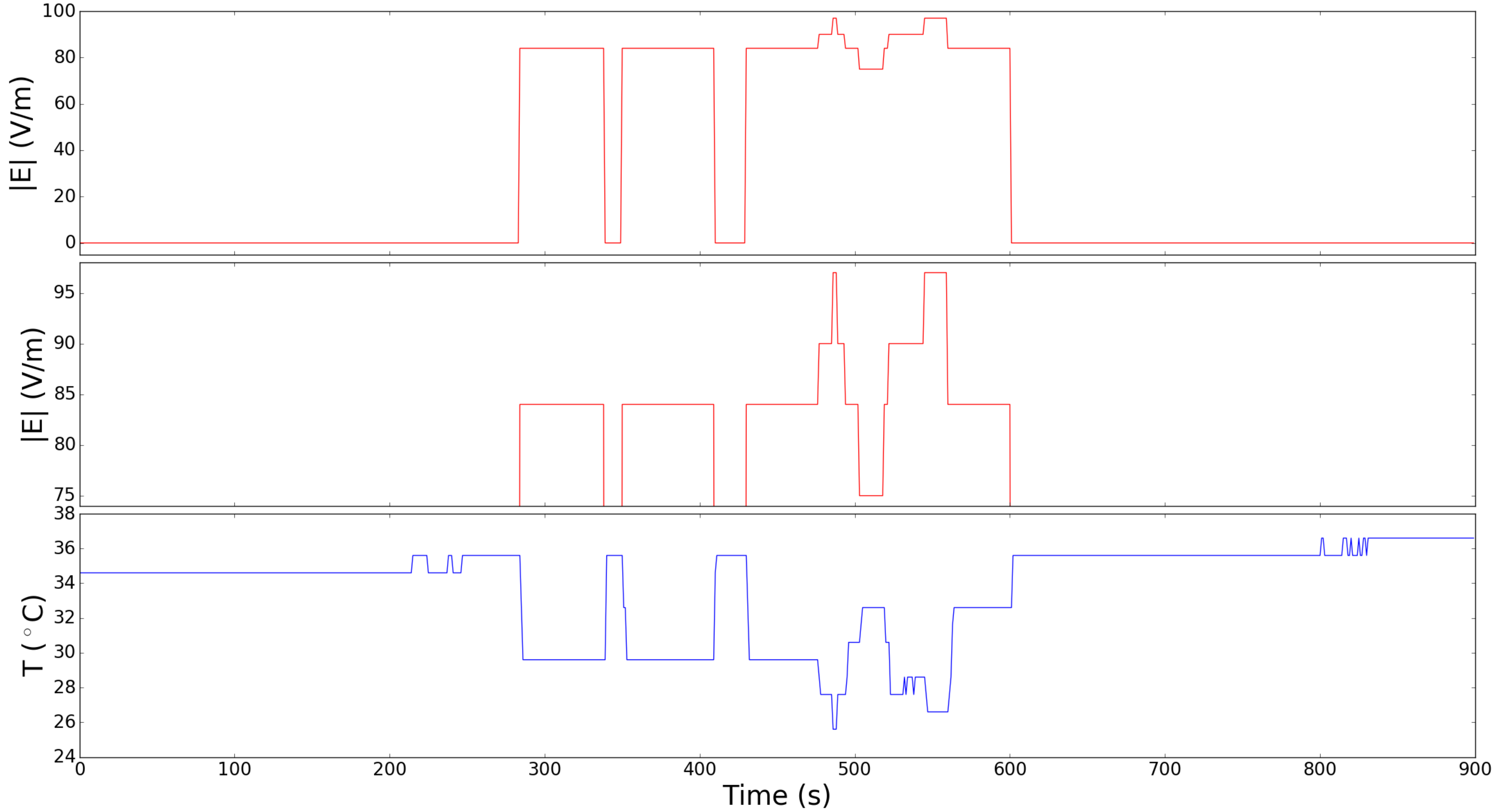
EFFECTS: WI-FI INTERFACE



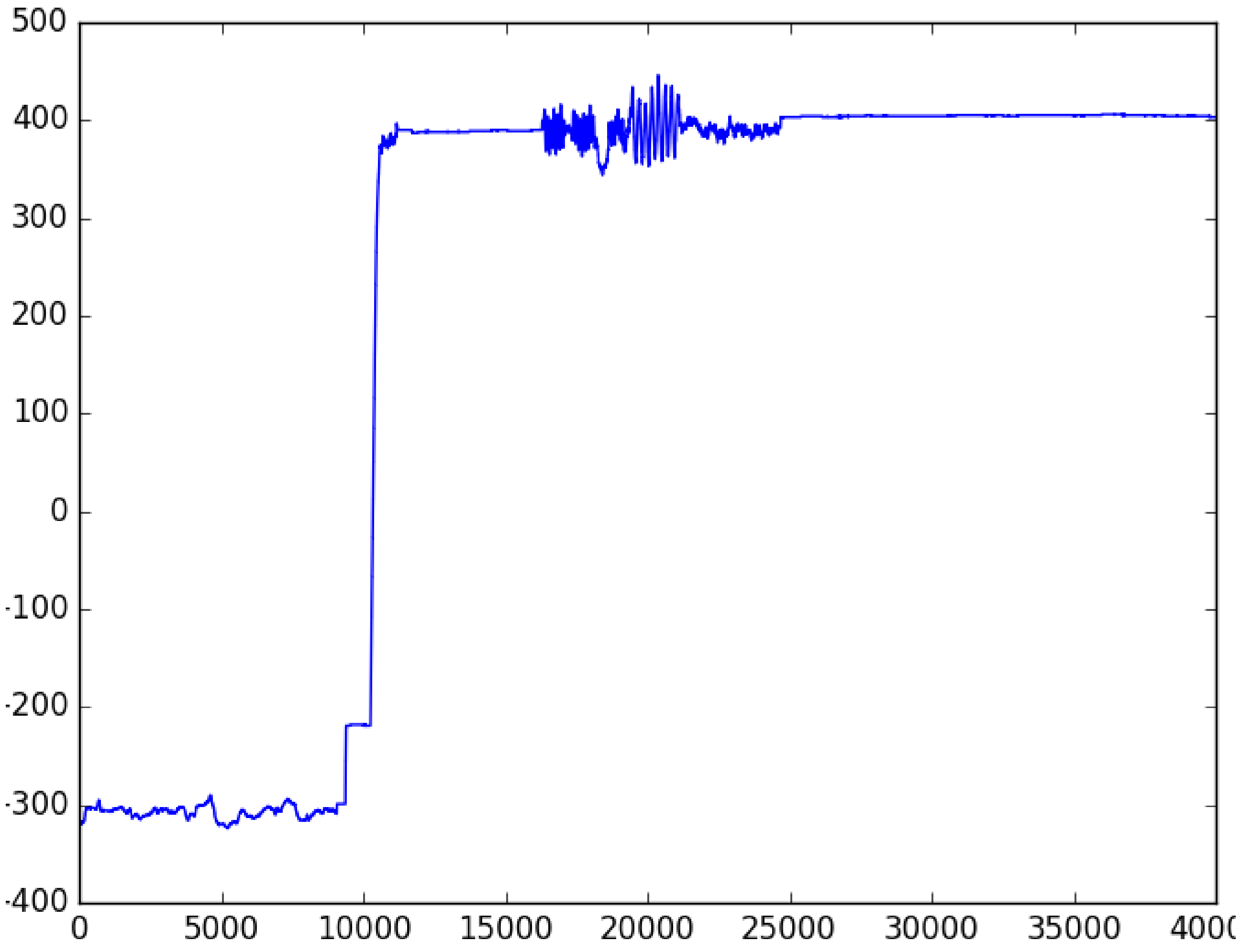
EFFECTS: HEIGHT

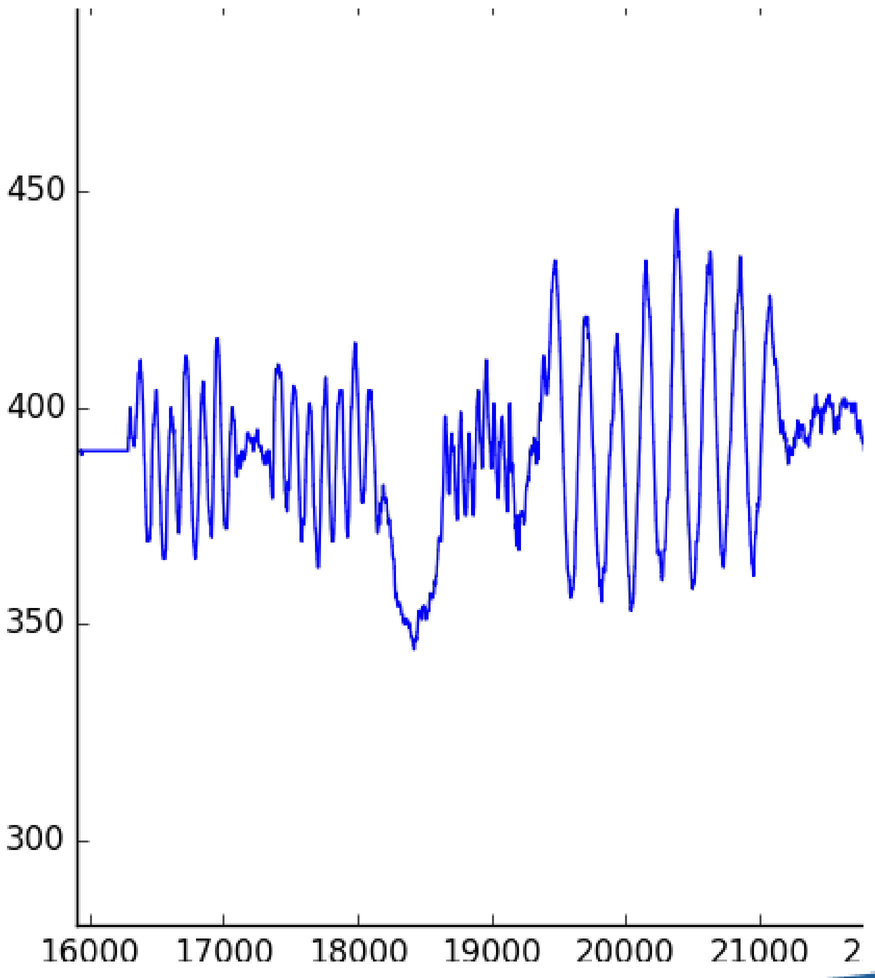


EFFECTS: BATTERY TEMPERATURE



EFFECTS: YAW ANGLE





EFFECTS: MISC

- Zeroing of the yaw value
- Embedded serial bus perturbation
- IMU SoC perturbation
- IMU calibration mode toggle

- Effects on the remote controller

Conclusion

CONCLUSION

- Proposed methodology is well adapted to COTS UAV
- Working on closed devices requires some agitlity
- Raw telemetry data is interesting

- Effects on IMU sensors can lead to flight path control
- Effects on battery can lead to emergency mode activation
- IEMI can lead to promising neutralization techniques

FURTHER WORK

- Relating effects to circuit topology could allow to understand underlying physical phenomena
- Diversify targets
- Investigating efficient hardening strategies
- More realistic conditions, model effect on feedback loop [9]
- Forensics
- Combined effects :
  - yaw control + height control for a fast response

Thank You

REFERENCES

1. DIEHL, “HPEMcounterUAS system,” online: http://drohnenabwehr.de/en/integrated-system/effectors/hpem/, accessed: 2018/01/30.
2. C. Adami, S. Chmel, M. Jöster, T. Pusch., and M. Suhrke, “Definition and Test of the Electromagnetic Immunity of UAS for First Responders,” Adv. Radio Science, 13, 3, November 2015, pp. 141-147, doi: 10.5194/ars-13-141-2015.
3. L. Torrero, P. Mollo, A. Molino, and A. Perotti, “RF immunity testing of an Unmanned Aerial Vehicle platform under strong EM field conditions,” in Antennas and Propagation (EuCAP), 2013 7th European Conference on, pp. 263–267, 2013.
4. Z. Tao, C. Yazhou, and C. Erwei, “Continuous wave radiation effects on UAV data link system in 2013 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference , pp. 321–324, 2013.
5. Q. Zhijun, P. Xuchao, H. Yong, C. Hong, S. Jie, Y. Cheng, “Damage of high power electromagnetic pulse to unmanned aerial vehicles,” High Power Laser and Particle Beams, vol. 29, no. 11, November 2017, doi: 10.11884/HPLPB201729.170216.
6. K. Sakharov, A. Sukhov, V. Ugolev, and Y. Gurevich, “Study of UWB Electromagnetic Pulse Impact on Commercial Unmanned Aerial Vehicle,” in 2018 International Symposium on Electromagnetic Compatibility (EMC Europe 2018), Amsterdam, Netherland, 2018.
7. C. Kasmi, J. Lopes-Esteves, “Automated analysis of the effects induced by radio-frequency pulses on embedded systems for EMC Functional Safety,” Radio Science Conference (URSI AT-RASC), 16-24 May 2015, doi: 10.1109/URSI-AT-RASC.2015.7303039.
8. A. Bolshev, How to fool an ADC, part II or attacks against sigma-delta data converters, Hardwear.io 2016
9. R. Gardner, “Pulse Injection of a Buck Converter,” 2nd Radio Science Conference (URSI AT-RASC), 28 May 2018

QUESTIONS ?

- José Lopes Esteves, jose.lopes-esteves@ssi.gouv.fr