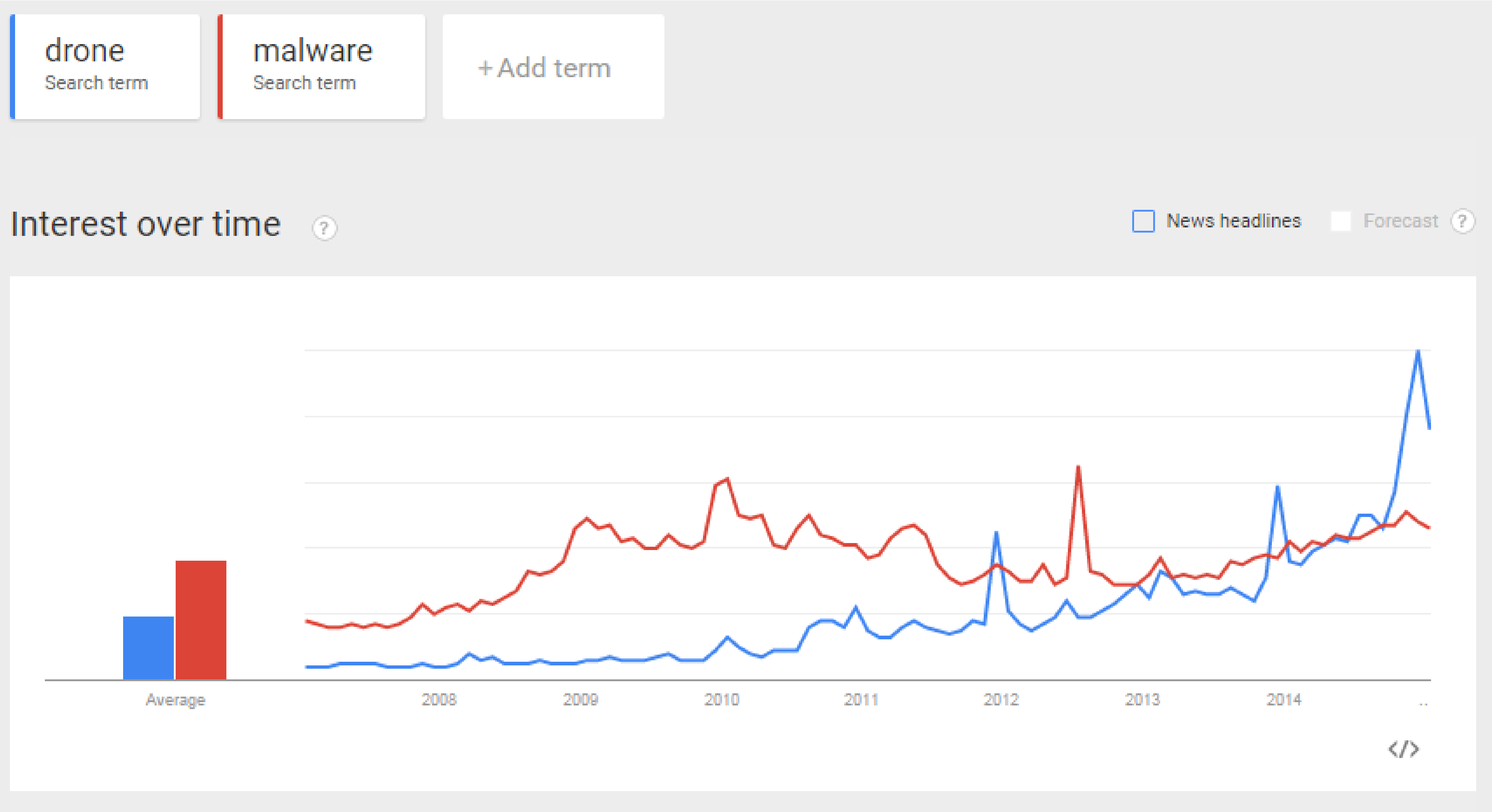
Attack on the drones

Vectors of attack on small unmanned aerial vehicles

Oleg Petrovsky / VB2015 Prague

Google trends



drone
Search term

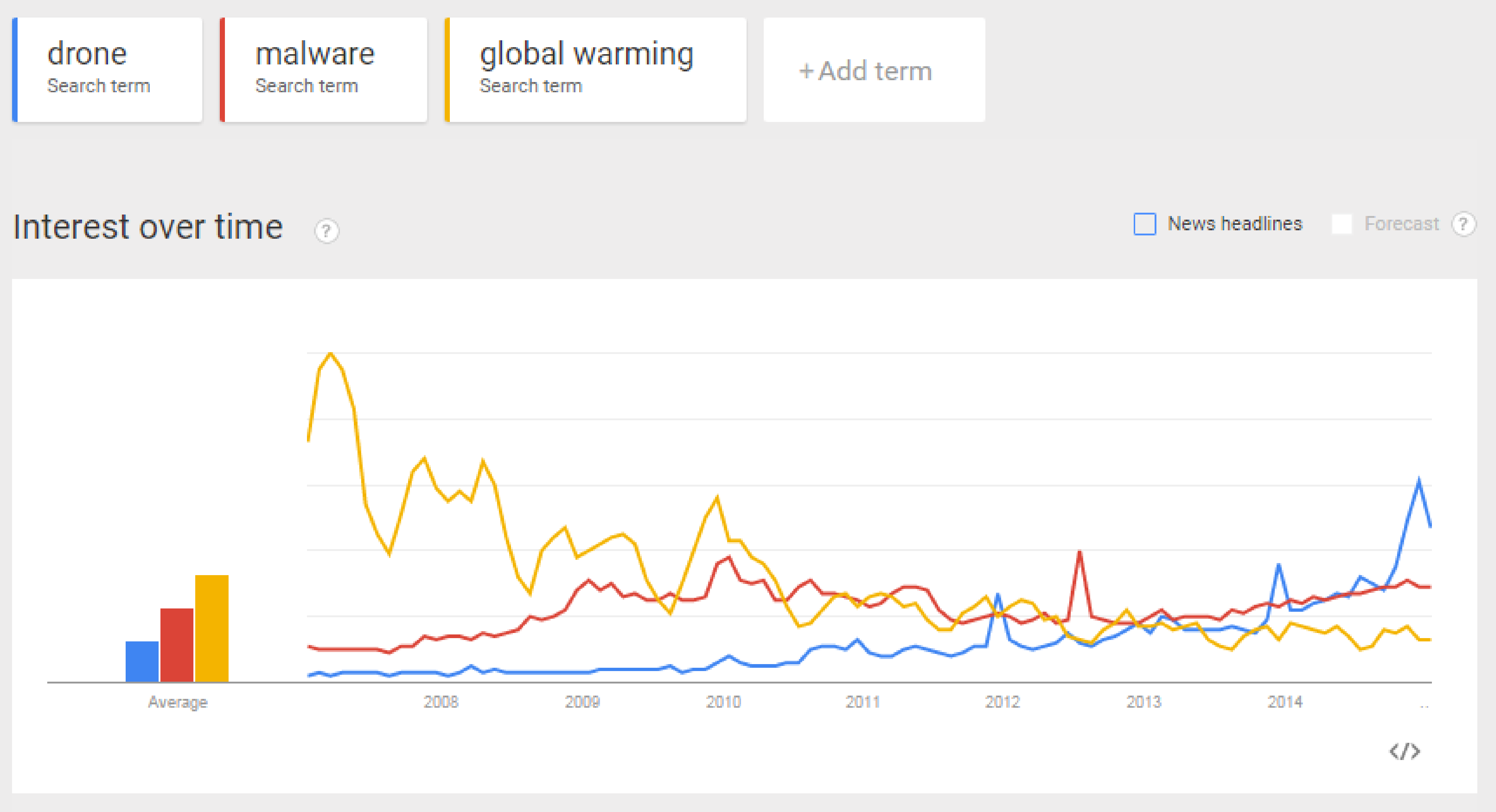
malware
Search term

+ Add term

Interest over time ?

□ News headlines □ Forecast ?

Google trends

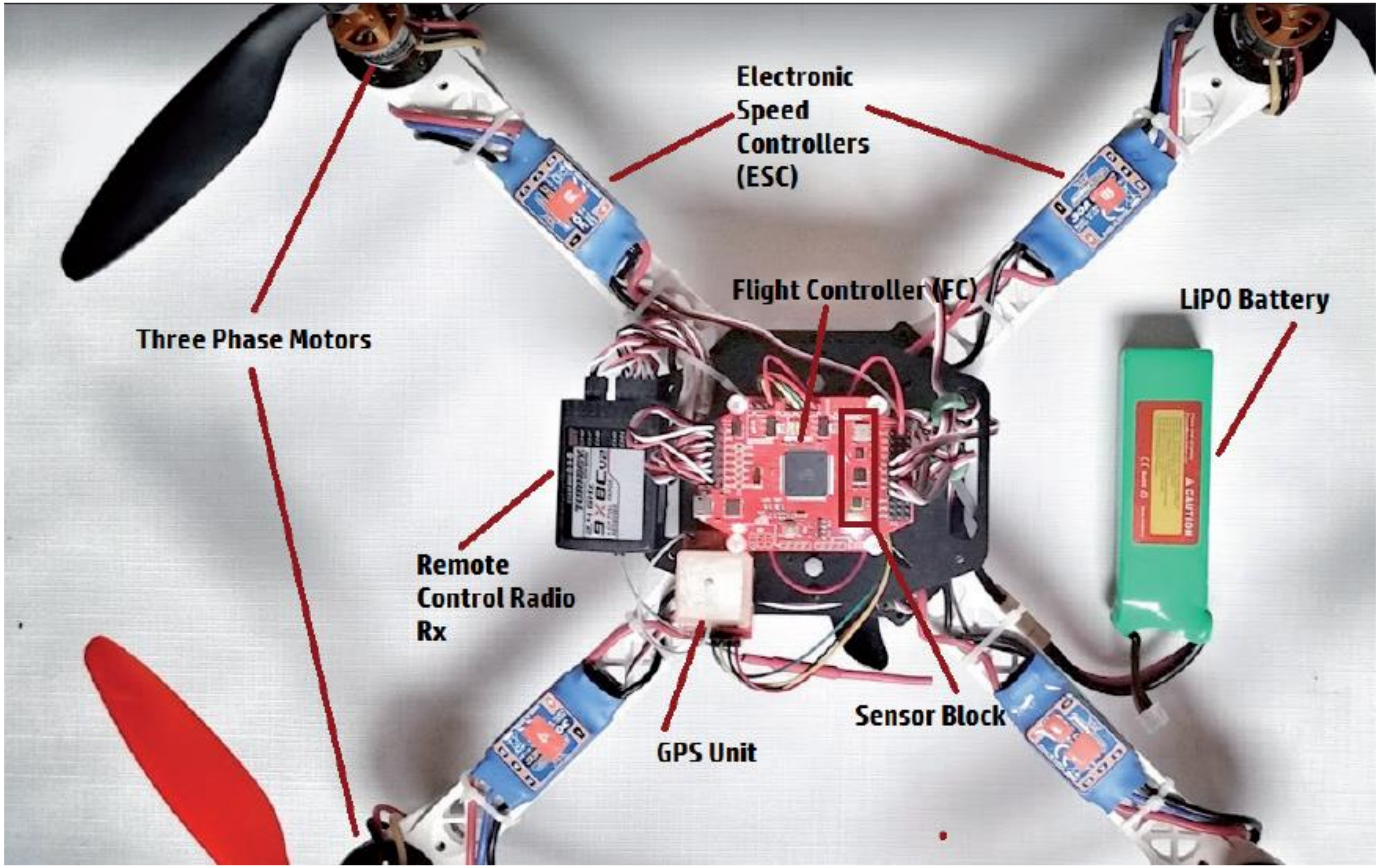


drone
Search term

malware
Search term

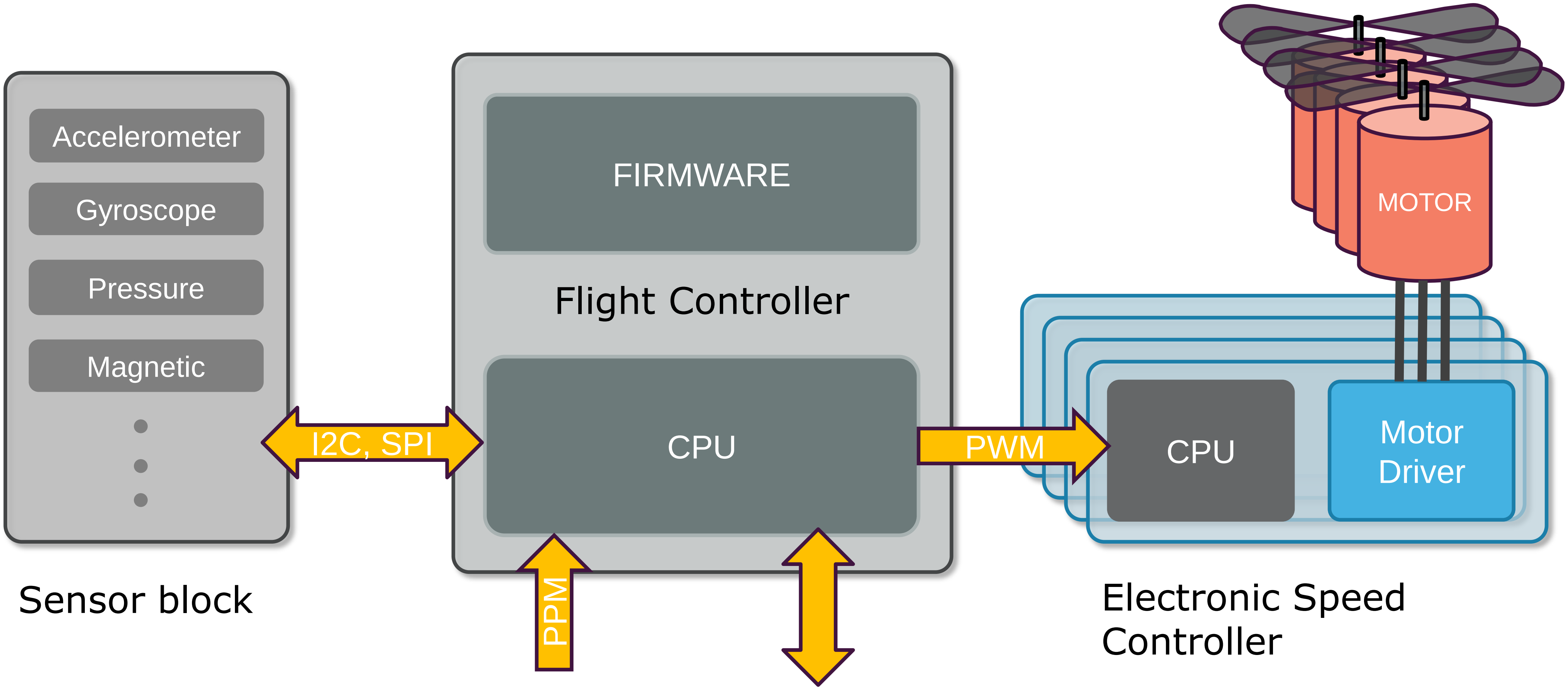
global warming
Search term

This is my drone. There are many like it, but this one is mine.



Majority of multi-rotor UAV follow the same design

Anatomy of a multi-rotor



Accelerometer

Gyroscope

Pressure

Magnetic

I2C, SPI

FIRMWARE

Flight Controller

CPU

PPM

PWM

CPU

Motor Driver

MOTOR

Sensor block

From a radio receiver

To and from Ground Control Station

Electronic Speed Controller

Sensor block

- Inertial measurement Units (IMU) sig degree of freedom in spatial orientation (3d-accelerometer, 3d-gyroscope)
- Magnetic orientation sensor
- Pressure sensor
- Global Positioning System
- All together up to 11 degrees of freedom
- Each unit is digitally controlled and has a network processor

Sensors glue logic protocols

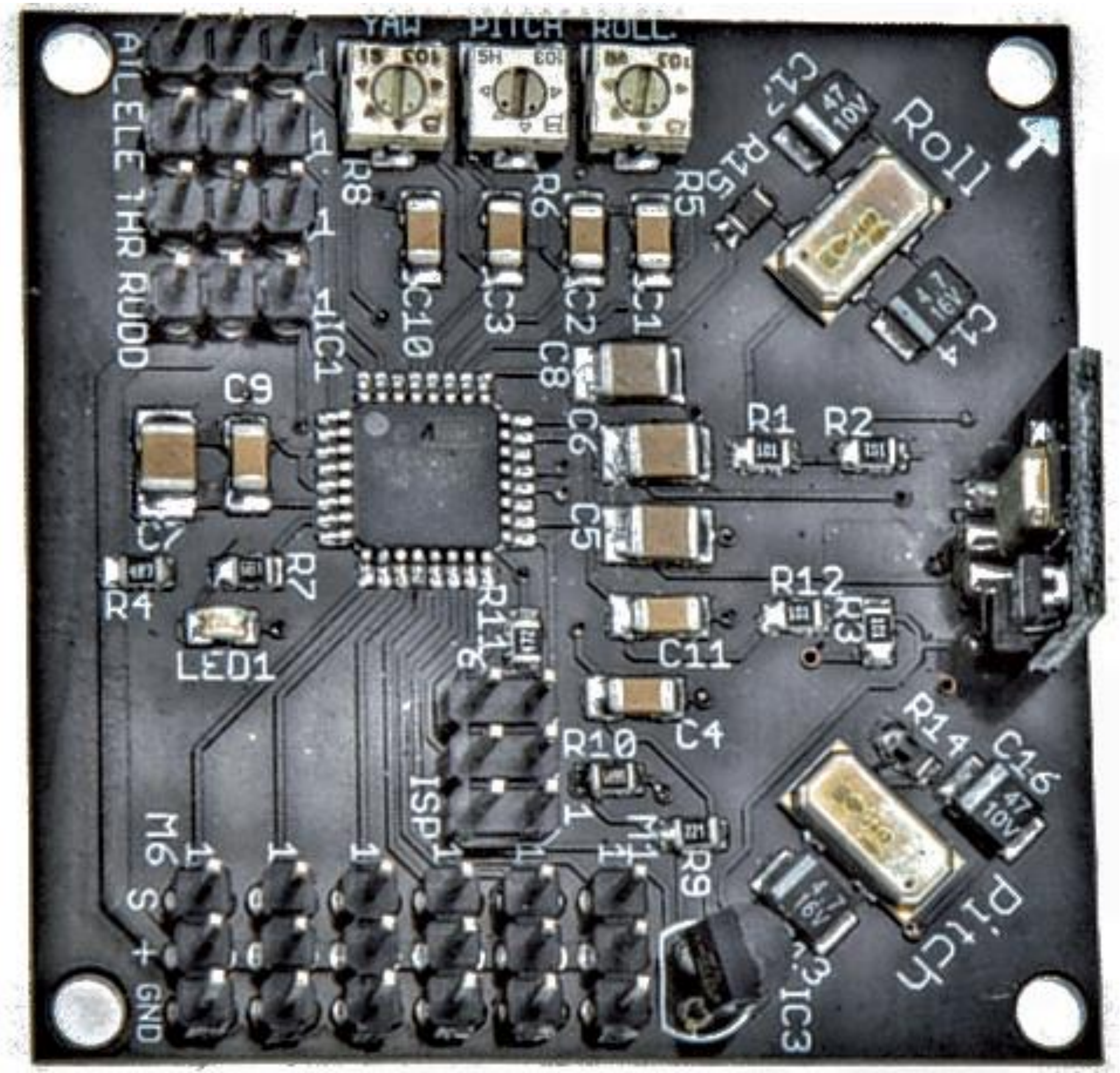
- I2C
- SPI
- UART

Daisy-chaining the sensors and using only two lines for communications highlights the I2C protocol as one of the preferable choices

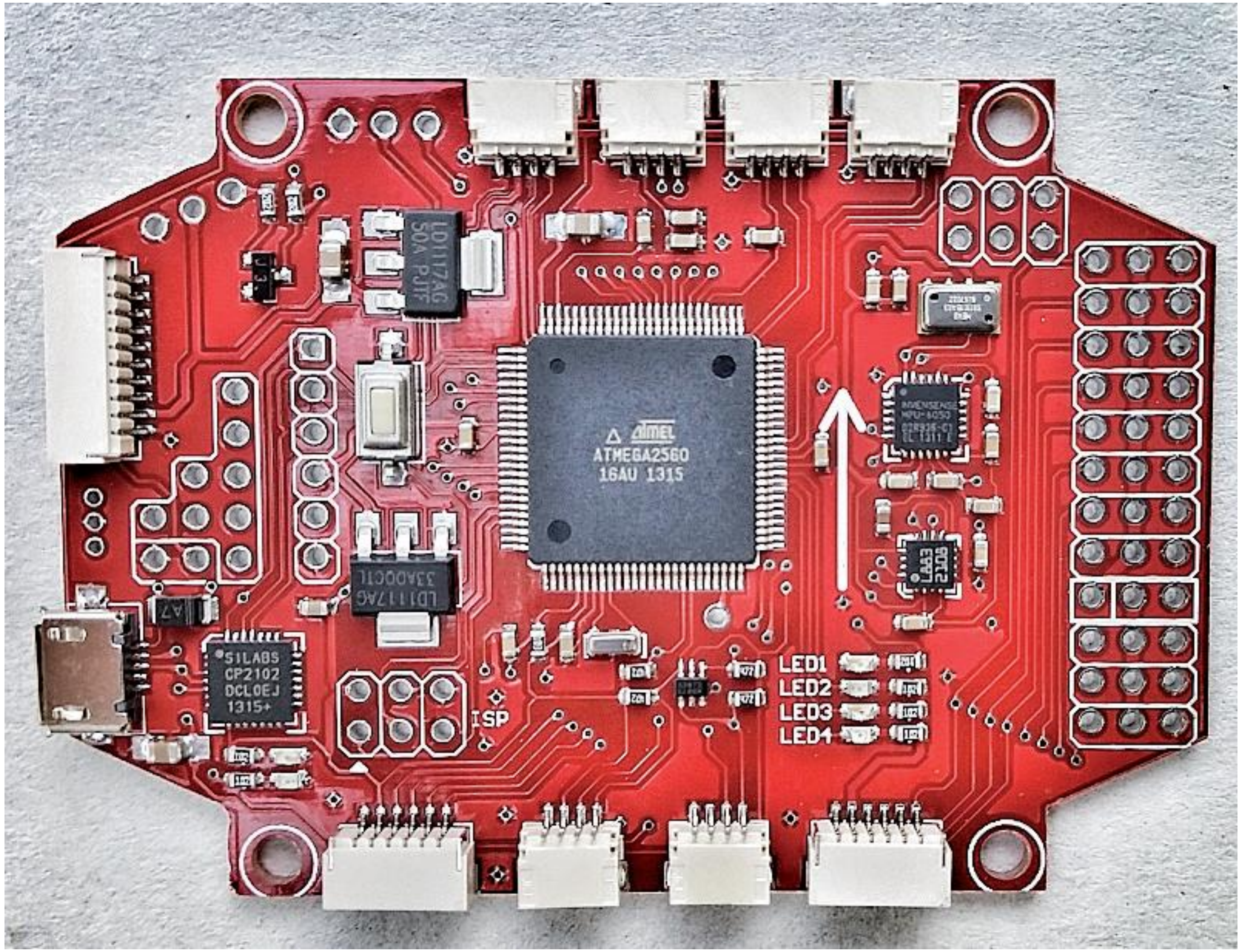
Popular flight controllers

KK

Rolf R. Bakke's (aka KapteinKuk) latest iteration is based on ATmega644 by Atmel sensor block based on IMU6050 (no default GPS, magnetic or barometric pressure sensors)



Popular flight controllers



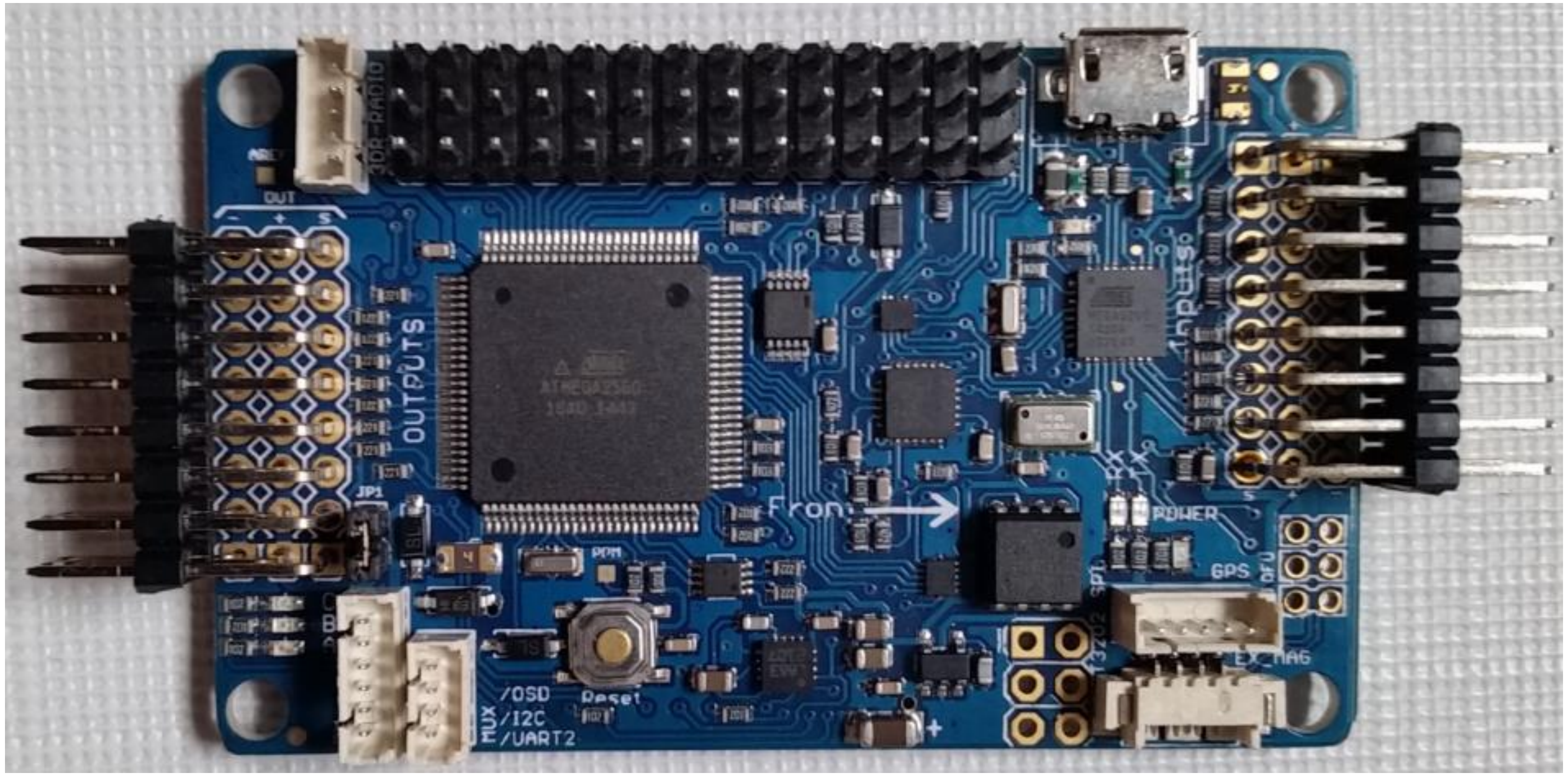
MultiWii

Earlier versions of the firmware relied on sensors found in the Nintendo Wii Nunchuck, firmware was originally written for 8-bit Atmel microcontrollers using the processing language in the Arduino framework utilizing open source under GNU GPL v3 and open hardware

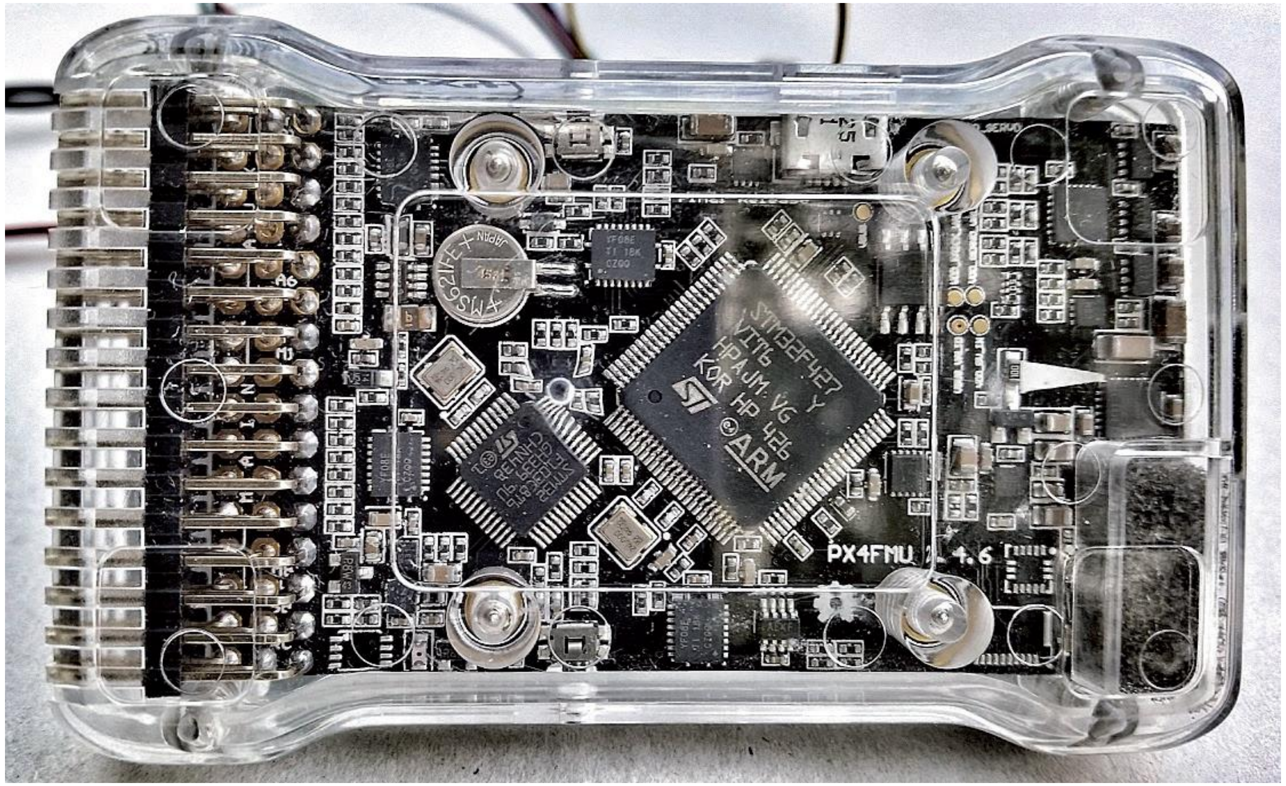
Popular flight controllers

APM by 3DRobotics

ArduPilotMega CPU ATmega2560, Sensors: IMU6050 3-axis accelerometer and gyroscope, MS5611 – barometric, HMC5883L magnetometer, can be connected to GPS



Popular flight controllers



3DRobotics PX4 Group

Pixhawk STM32F4 Cortex M4 series CPU and has a second STM32F1 CPU as a failsafe option. Sensor module, the InvenSence MPU6000 three-axis accelerometer gyroscope. 14-bit STM LSM303D accelerometer and magnetometer, the STM L3GD20 three-axis 16-bit gyroscope MS5611 barometer.

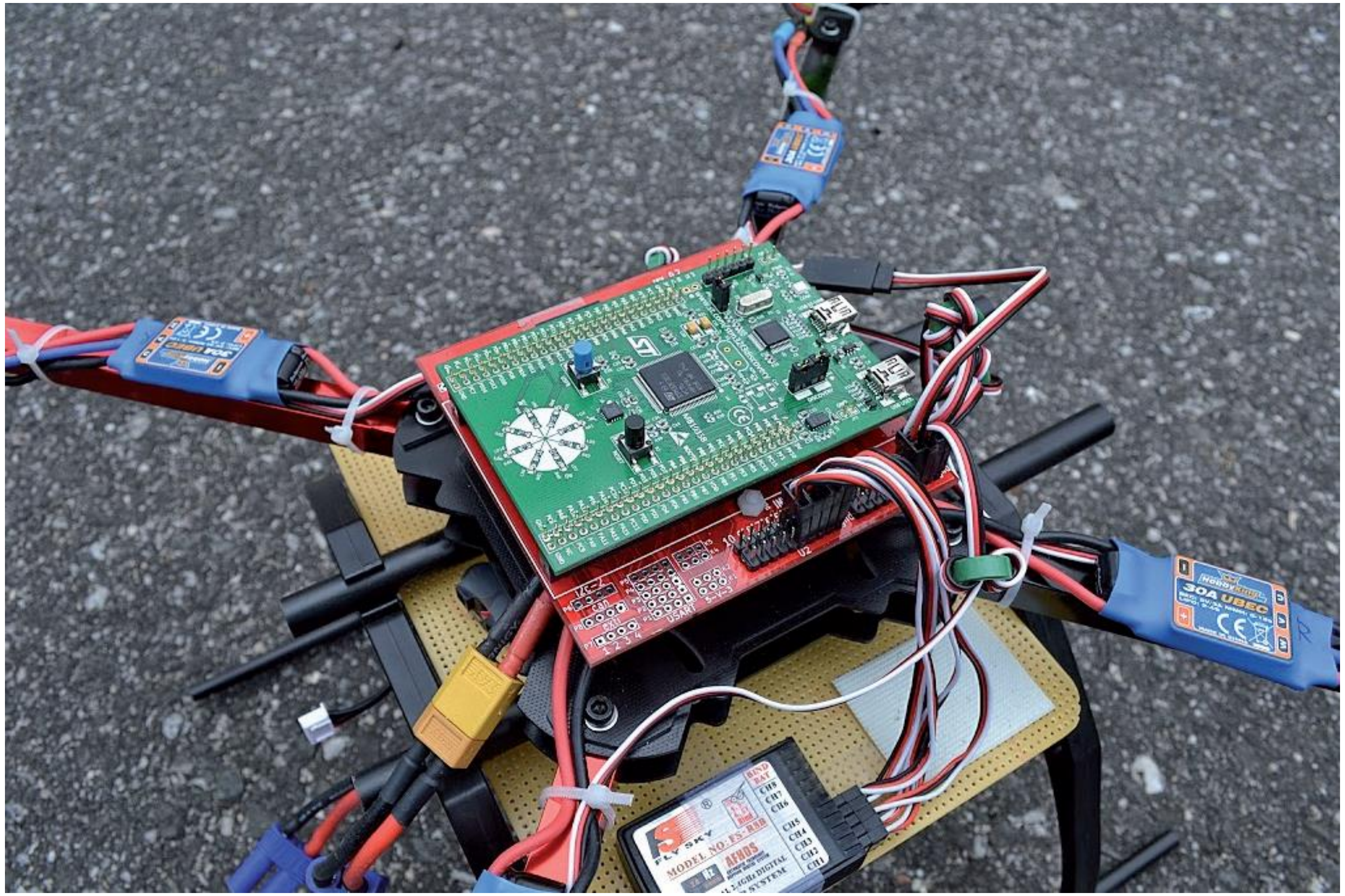
Popular flight controllers

Open Pilot

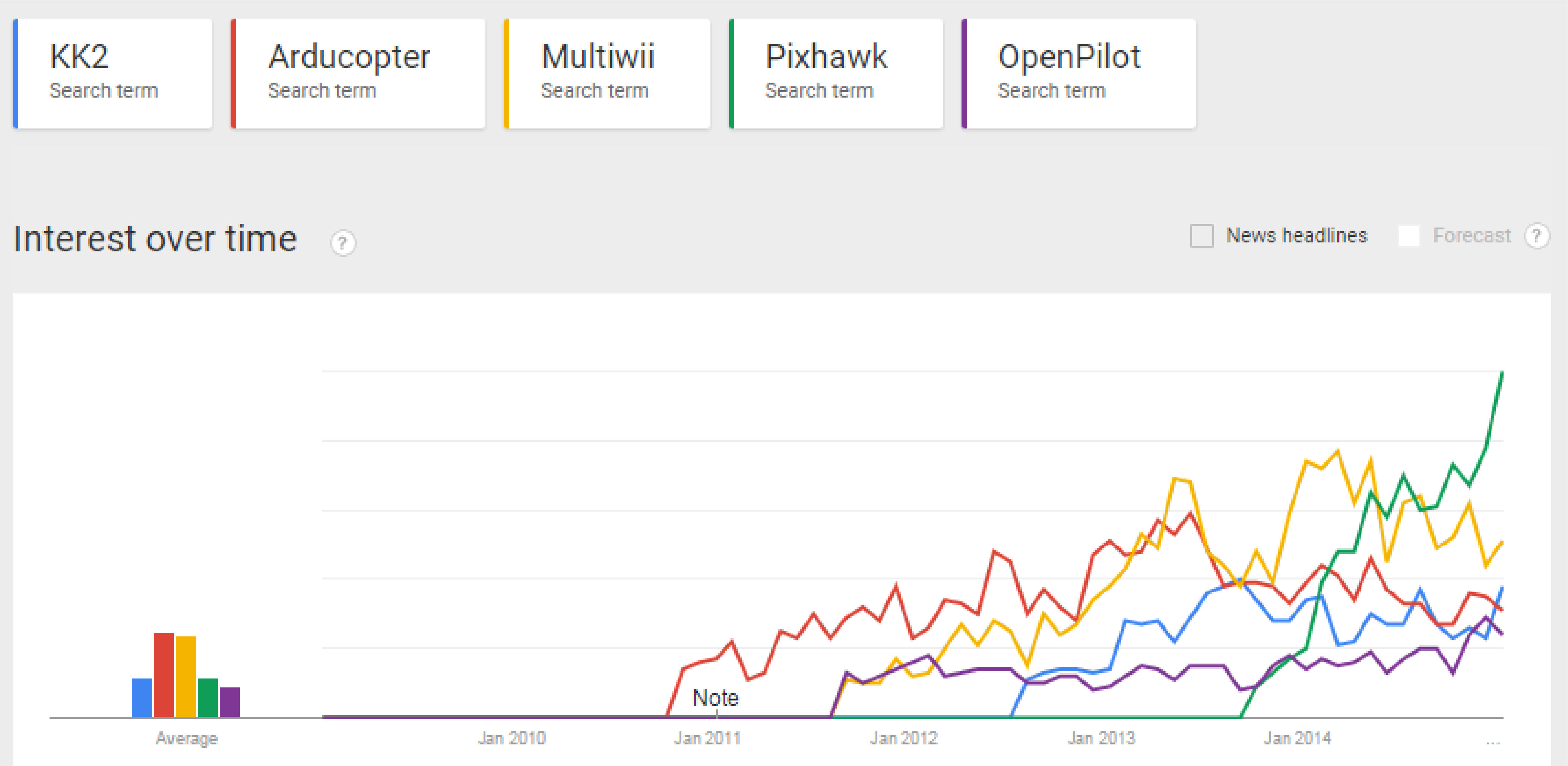
CC3D and Revolution CPU
STM32F1, STM32F4
sensors: IMU6000,
IMU6050

TauLabs

Fork to support STM32F3,
STM32F4 popular
development boards
Discovery F3, *Discovery F4*



Google trends



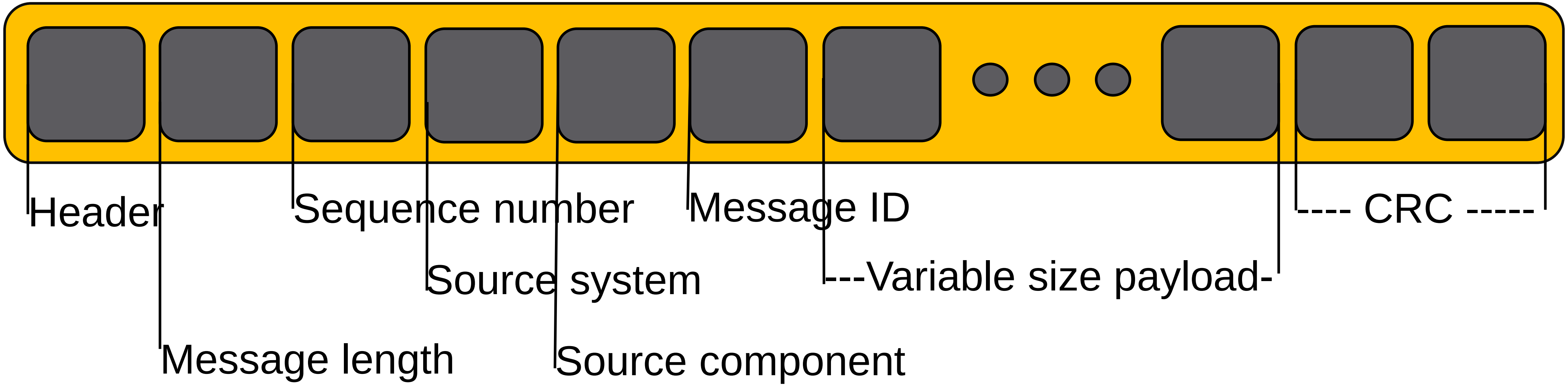
Ground Control Station

- Communicates with UAV via wired or wireless telemetry
- Displays real-time data on the UAVs performance and position serving as a “virtual cockpit”
- A GCS can also be used to control a UAV in flight
- Uploads new mission commands and sets parameters
- Use of Joystick or Gamepad to control multi-rotor (http://copter.ardupilot.com/wiki/common-optional-hardware/flying-with-a-joystickgamepad-instead-of-rc-controller/)

Telemetry and Control Protocols

- Are very lightweight, header-only message protocols (most of the time)
- Designed efficiently to transfer packed C-structures over serial channels and provide a communication layer to and from the ground control station
- Are fast, low overhead and are not secure (most of the time)
- Secure layer is expected from the transport protocols (sub Ghz or WiFi radio communications layer)

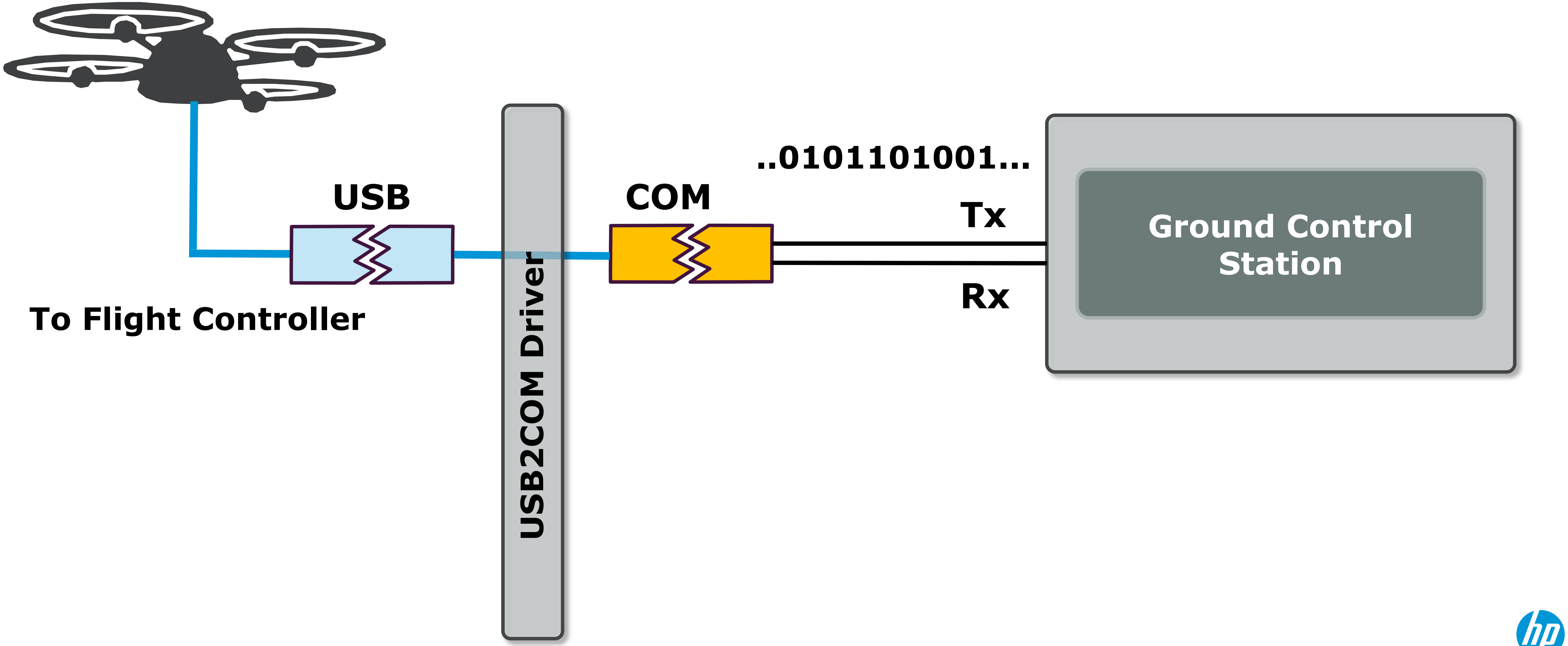
Telemetry and Control Protocols



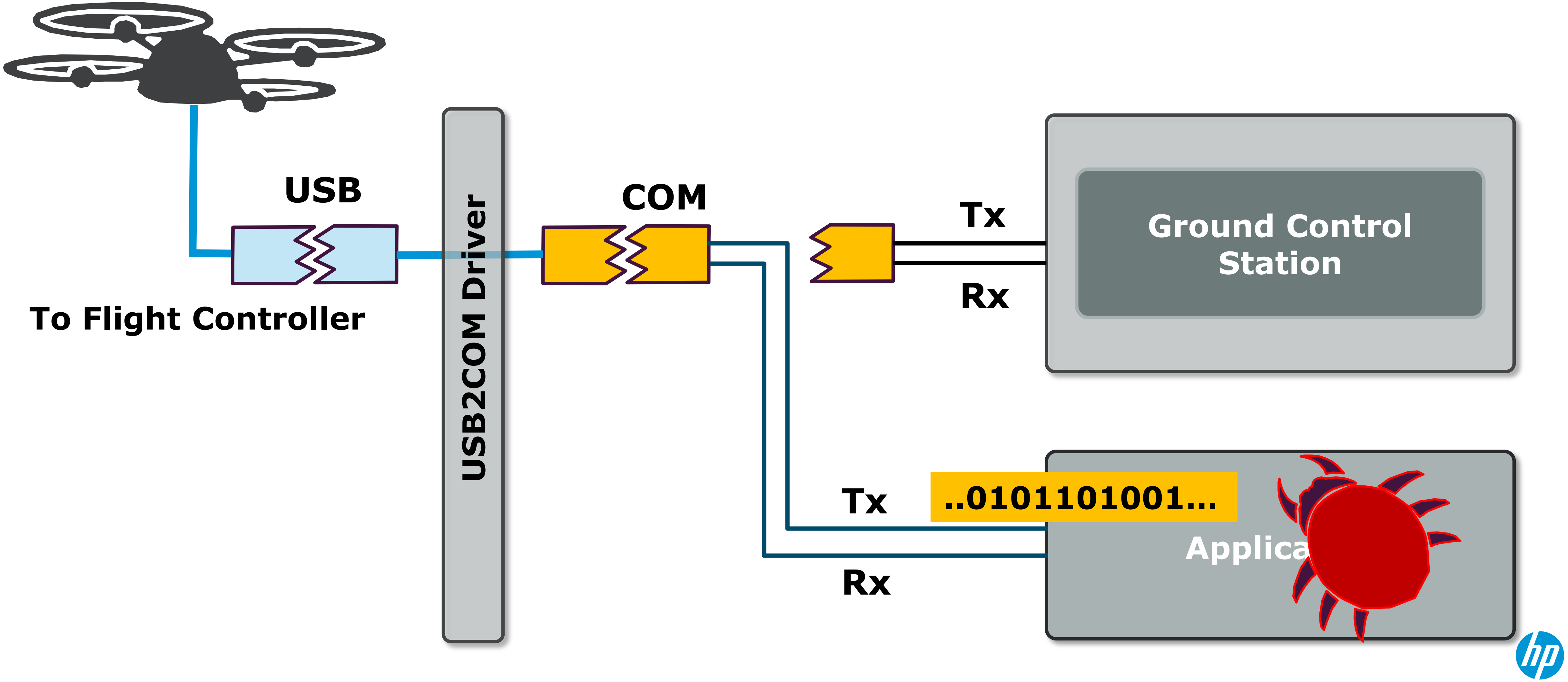
Firmware upgrades

- Firmware updates rely on bootloaders
- Firmware, in most cases, is not signed
- Firmware is uploaded through a serial or USB link
- Triggers to upload firmware are software driven (for instance DTR of a serial port or slow baud rate)
- Firmware can be modified and uploaded to a flight controller to alter its behavior

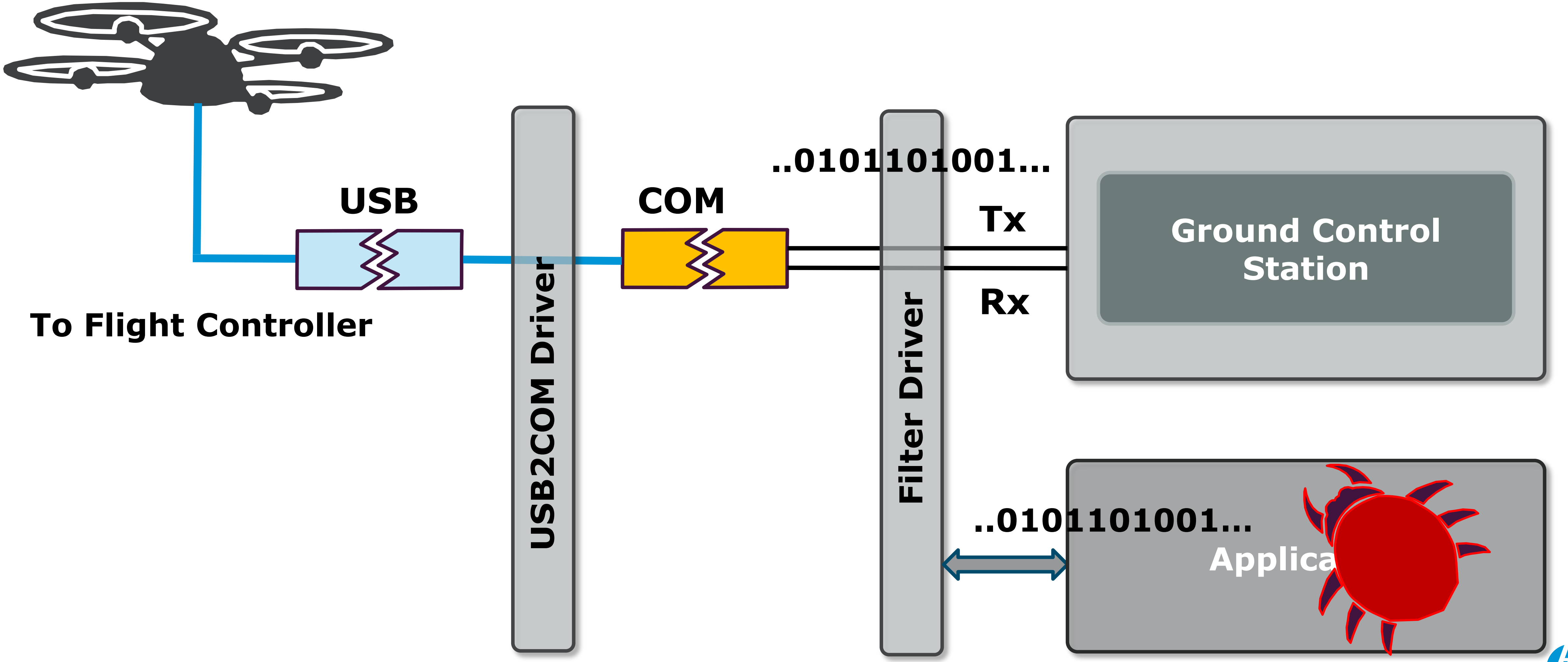
Flight Controller to Ground Station communication



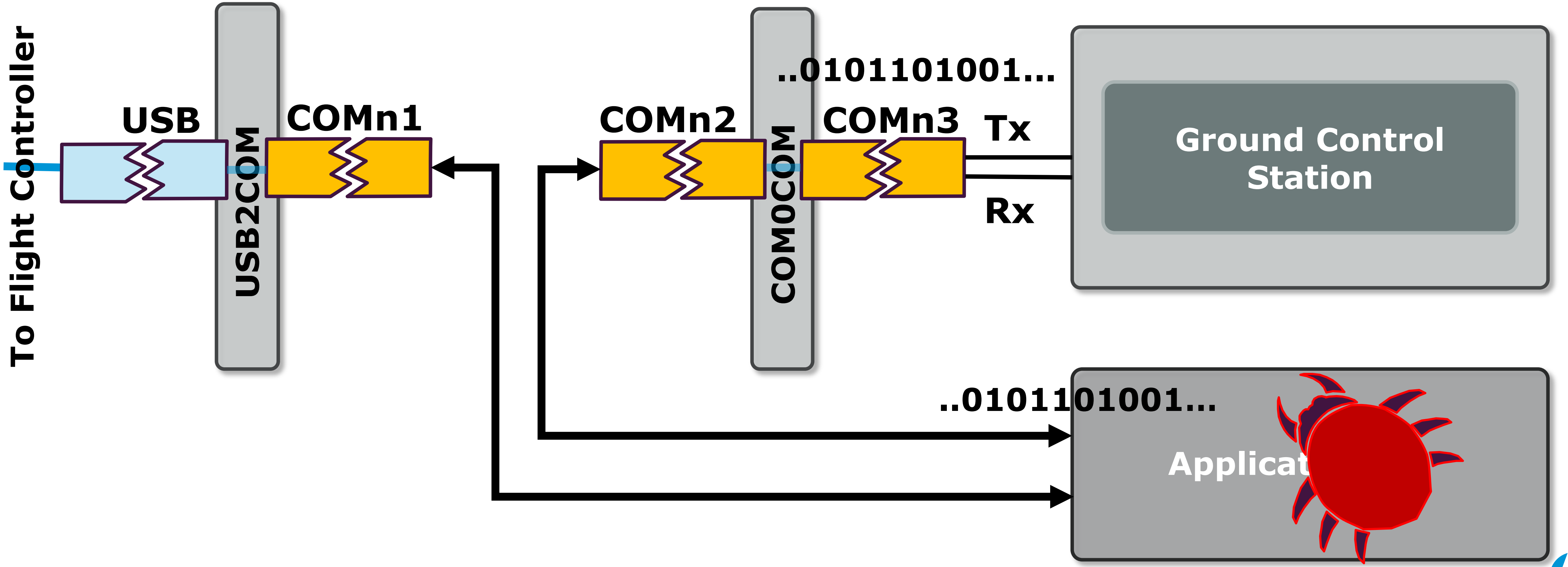
COM Port Flight Controller communication



Flight Controller to Ground Station communication



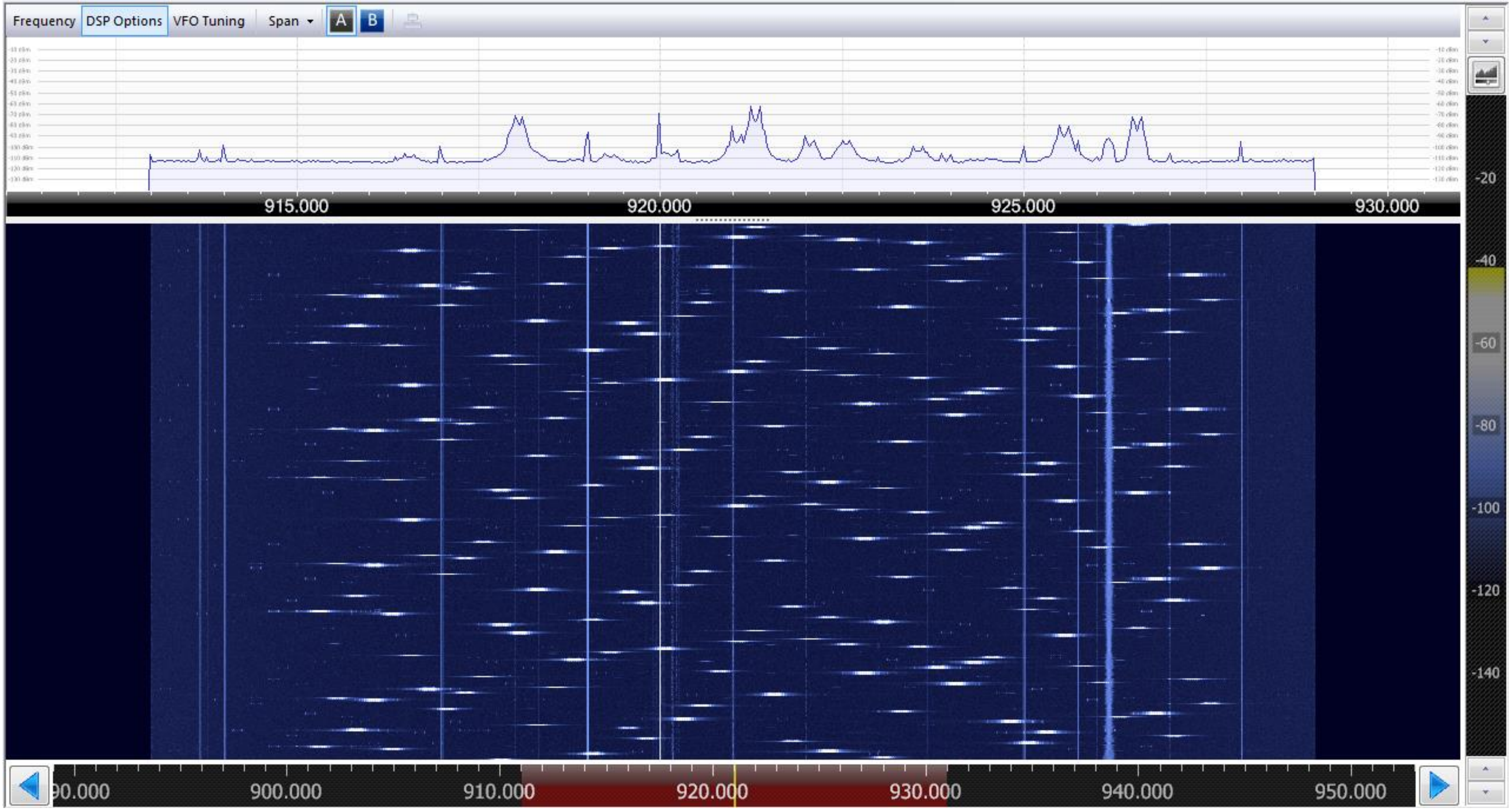
Flight Controller to Ground Station COM0COM intercept



Breaking into a transport link

- WiFi (IEEE 802.11b,g,n,ac)
- BlueTooth (IEEE 802.15.1, v2.1)
- ISM band Radio Frequency integrated circuits 3DR Radio (Si1000,Si4332 433 or 915Mhz), OpenLRS (RFM22B 433Mhz)
- The transport link implementation for the 3DR Radio uses a variety of a spread spectrum technology such as frequency hopping (FHSS) and time division multiplexing(TDM). The channel sequencing is based on NETID. Within a channel the radio uses Gaussian Frequency Shift Keying (GFSK) modulation
- Not easy but can be done

Spectrum of the telemetry link over ISM band



Conclusion

- Shift towards more powerful hardware platforms in embedded designs
- We are witnessing an increase in drone research and development across various types of industries
- Consideration has to be given to securing firmware on embedded UAV modules.
- The use of secure boot loaders and mechanisms of firmware authentication and encryption has to become ubiquitous.
- Attention has to be given to the uses of encryption for wireless control and telemetry protocols.

Thank you

hp.com/go/hpsr