UAV Systems and Security

Stuart MacIntosh aka barf

SAFETY

- $F = \frac{1}{2} m \cdot v^2$
- Learn real aviation standard operating procedures (SOPs)
- RIP Roman Pirozek
- Death or injury can result
  - don't war-hack other ppls drones, centrifuges, pacemakers, et cetera; disclaimation disclaimed

Nomenclature

Fancy word for 'words used'

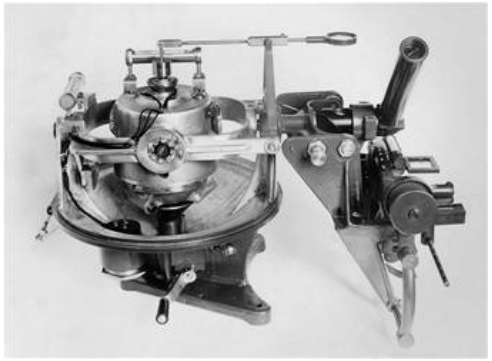
- **Remotely Piloted Vehicle (RPV)**
  - Radio Control (RC) planes and man-sized toys
  - aka **First Person View** (FPV) flight
  - Fun

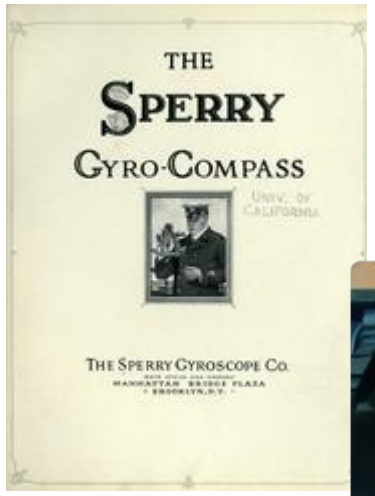
- **Unmanned Aerial/Autonomous Vehicle/System (UAV / UAS)**
  - Look anything like RC to real planes
  - Autonomous navigation
    - takeoff, waypoints, loiter, landing, etc
  - RPV/FPV flight capable, for safety reasons
  - Follows a Flight Plan

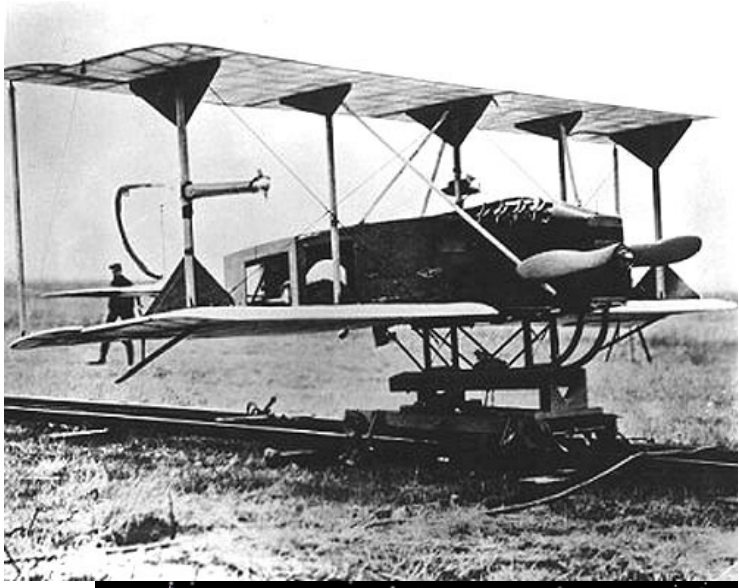
Flight School

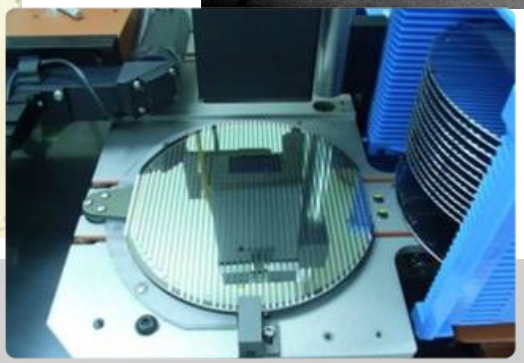
- Fixed-wing
  - As opposed to flapping-wing (ornithopter)
- Rotary-wing
  - N-copters (quad, hexacopter, octacopter, etc)
  - Helicopters
- Lift, Drag, Stall, Air masses & energy management
- Radio navigation
- Dead reckoning

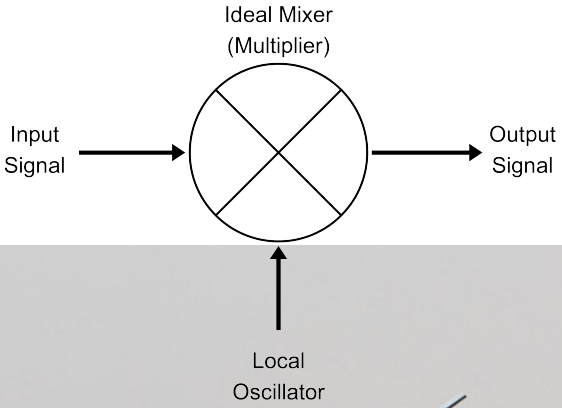
History




THE
SPERRY
GYRO-COMPASS
THE SPERRY GYROSCOPE CO.





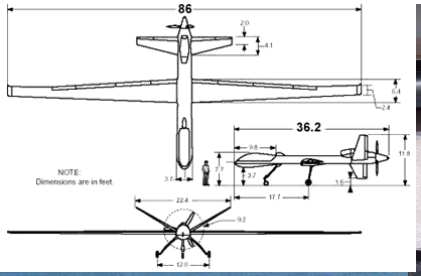

Ideal Mixer
(Multiplier)
Input
Signal
Output
Signal
Local
Oscillator

UAV : military

- Example US MILSPEC nomenclature:
  - RQ-4 “GlobalHawk”
  - RQ-21 “ScanEagle” - 1x gifted to Iran
  - MQ-8 “FireScout” - LibyaFailScout?
  - MQ-9 “Reaper” - some lost in Afghanistan
- Shares/sometimes is civilian/commercial technology, aka commercial off-the-shelf sourcing (COTS)
- Lots in common with commercial UAV tech anyway
- Big hardware catalog & lotsa MILSPEC tech pr0n selfies online
- Empirical performance data
- System designs given away in sales material
- Purpose: war

War

- If you thought John Connor needed protecting from Terminators, imagine how Afghanis feel about their kids...
- Therefore; Terminator was phrophecy, also a movie



UAV : civillian / commercial

- Has a lot in common with the DIY stuff
- Individuals to Aviation industry heavyweights
- We see COTS UAVs used today for
  - Aerial photography and film
  - Science, research and education
  - First responders, Police, Fire, Search and rescue
  - Industry (only for agriculture here in NZ, AFAIK)
  - Please tell me if you know any others!

Hobby-spec == Commercial-spec?

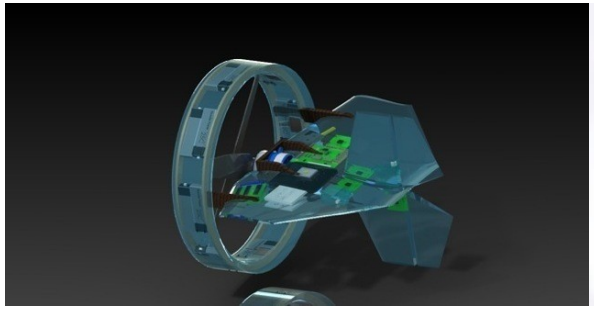
- Is that Futaba radio gear?

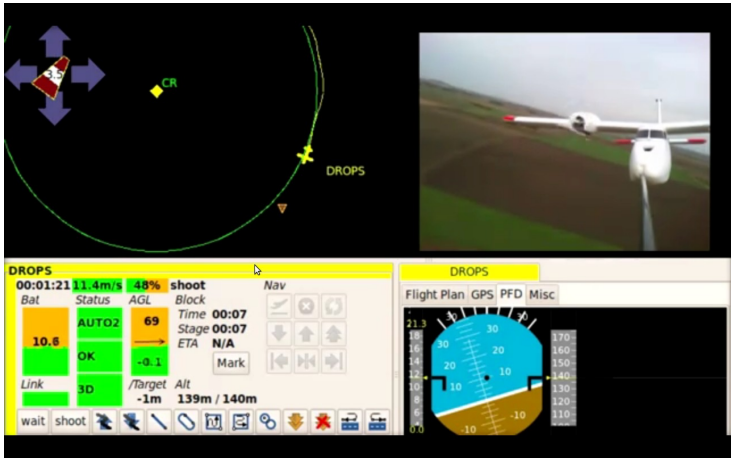
Open Source UAS

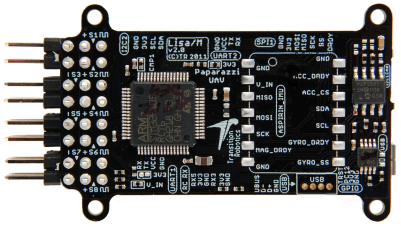
- GPL, BSD and various
  - Paparazzi. ARM7 STM32 and LPC21xx based
  - PX4. ARM7 STM32, NuttX, RTOS
  - OpenPilot. ARM7 STM32
  - ArduPilot. Pushing the limits of 8-bit AVRs!
  - All the others I'm missing(?)

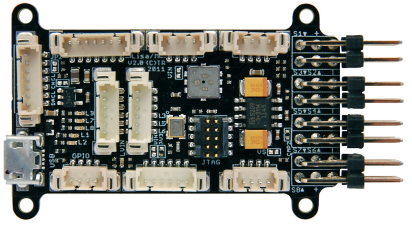
Paparazzi

- GNU GPL hardware and software, with plenty of git activity, forks
- GNU Mailman mailing list!
- IMHO the most mature and professional Open Source autopilot
- MacOS X and GNU/Linux Ground Control Software
- Various hardware supported
- Community vendors

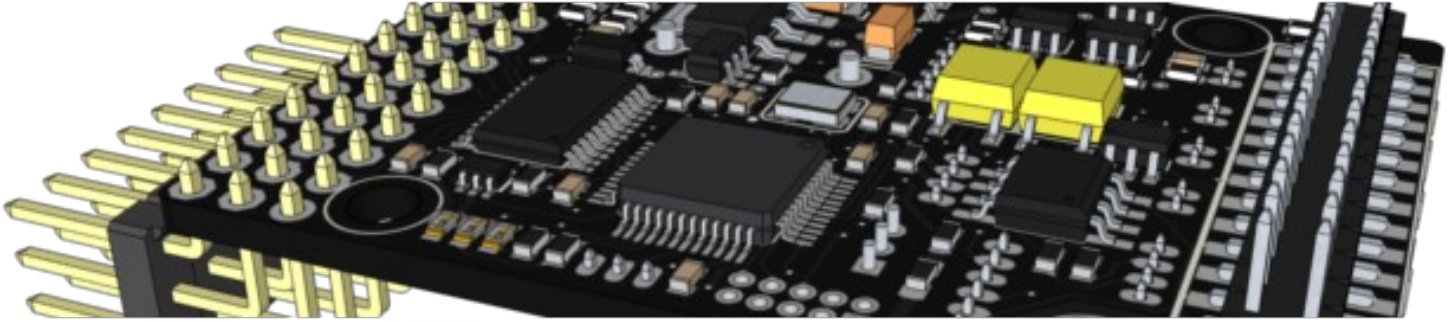


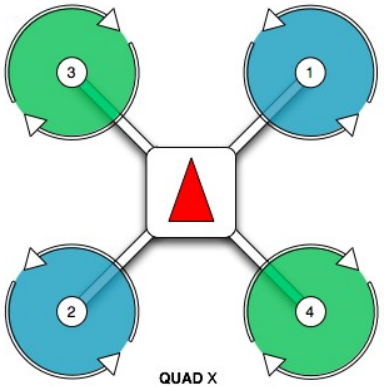






PX4 autopilot





Pixhawk PX4

Cool Open Source project started by:
Computer Vision and Geometry Group at ETH University, Zurich

- Open Source (BSD) Hardware and Software
- High quality, professional design
- Growing user base and vendor list
- Plugs into Parrot ARDrone even
- Uses NuttX RTOS, POSIX shiz

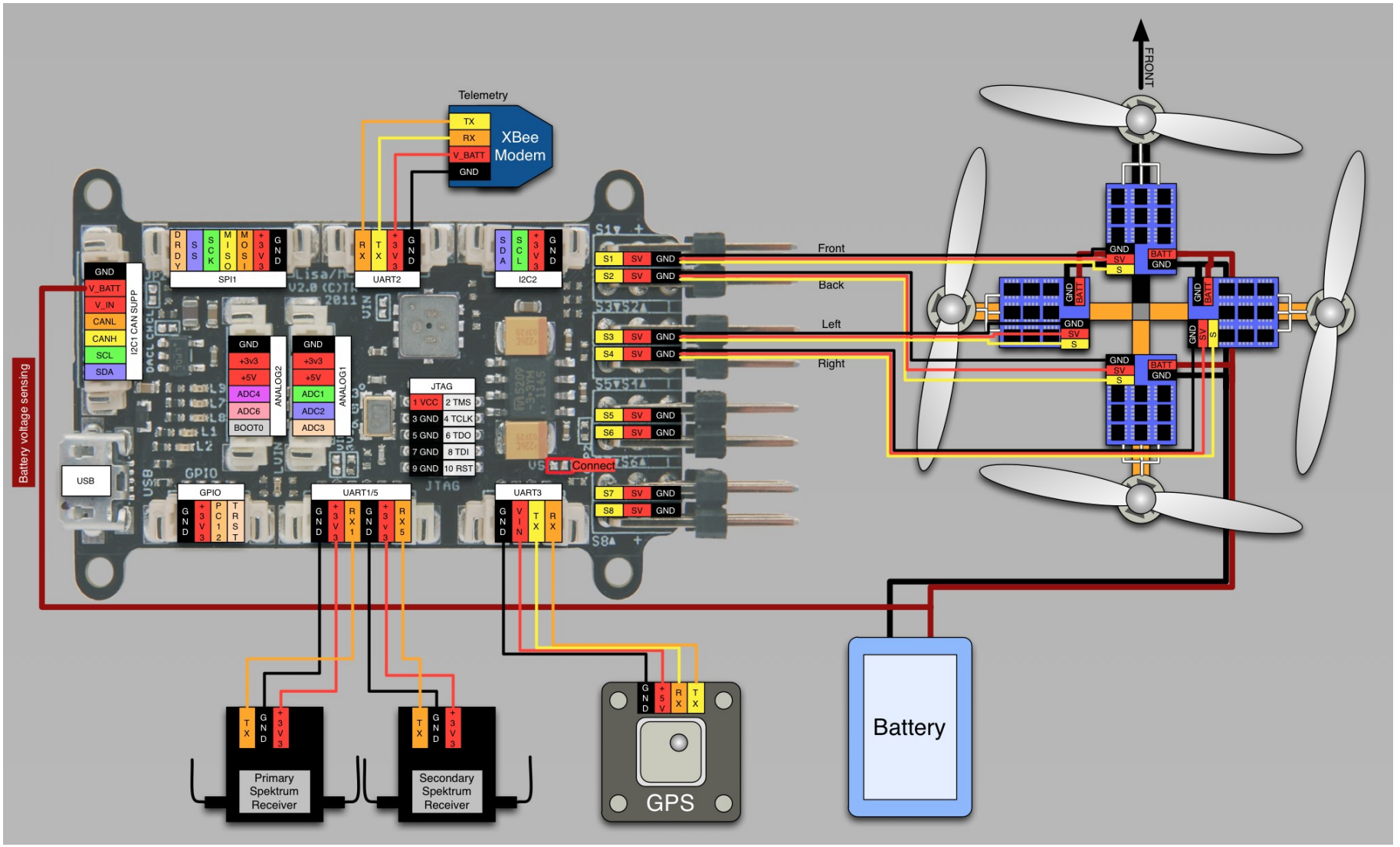
openpilot

Cute Own logo
Forums
Growing

ArduPilot

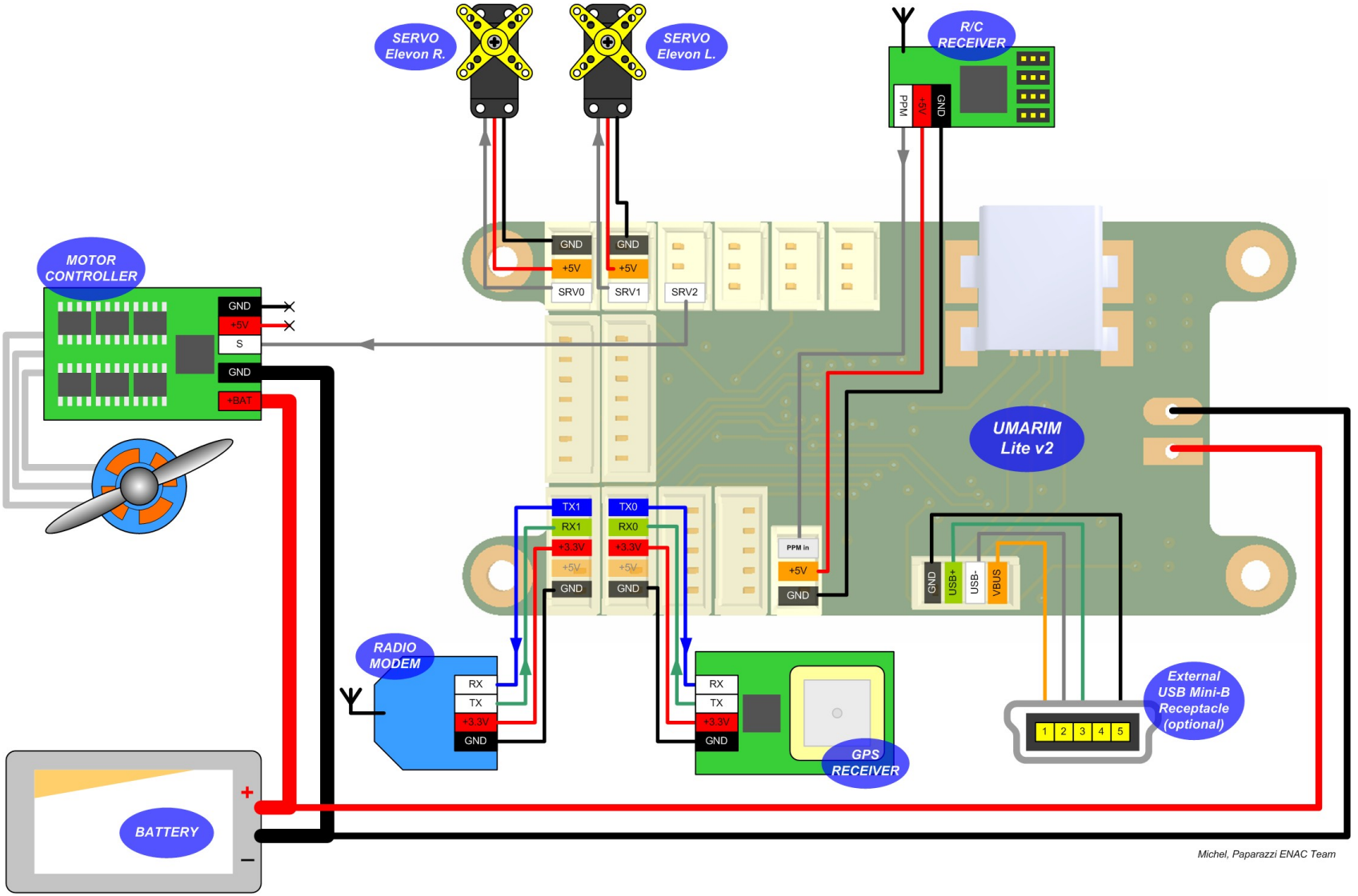
Generic System Diagram

- Multi-rotor-craft (heli is similar)



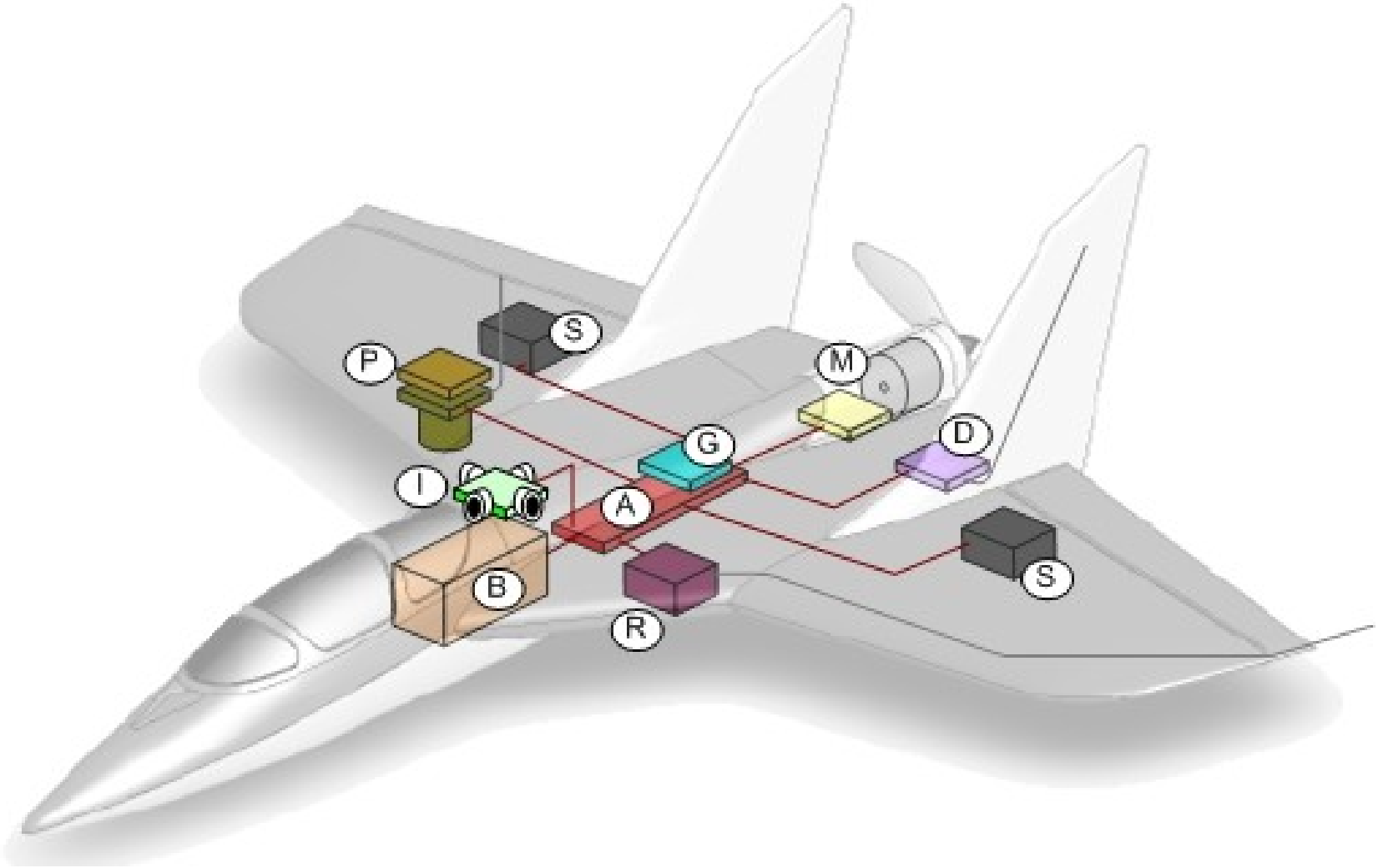
Generic System Diagram

- Fixed-wing RC aeroplane (Elevons)



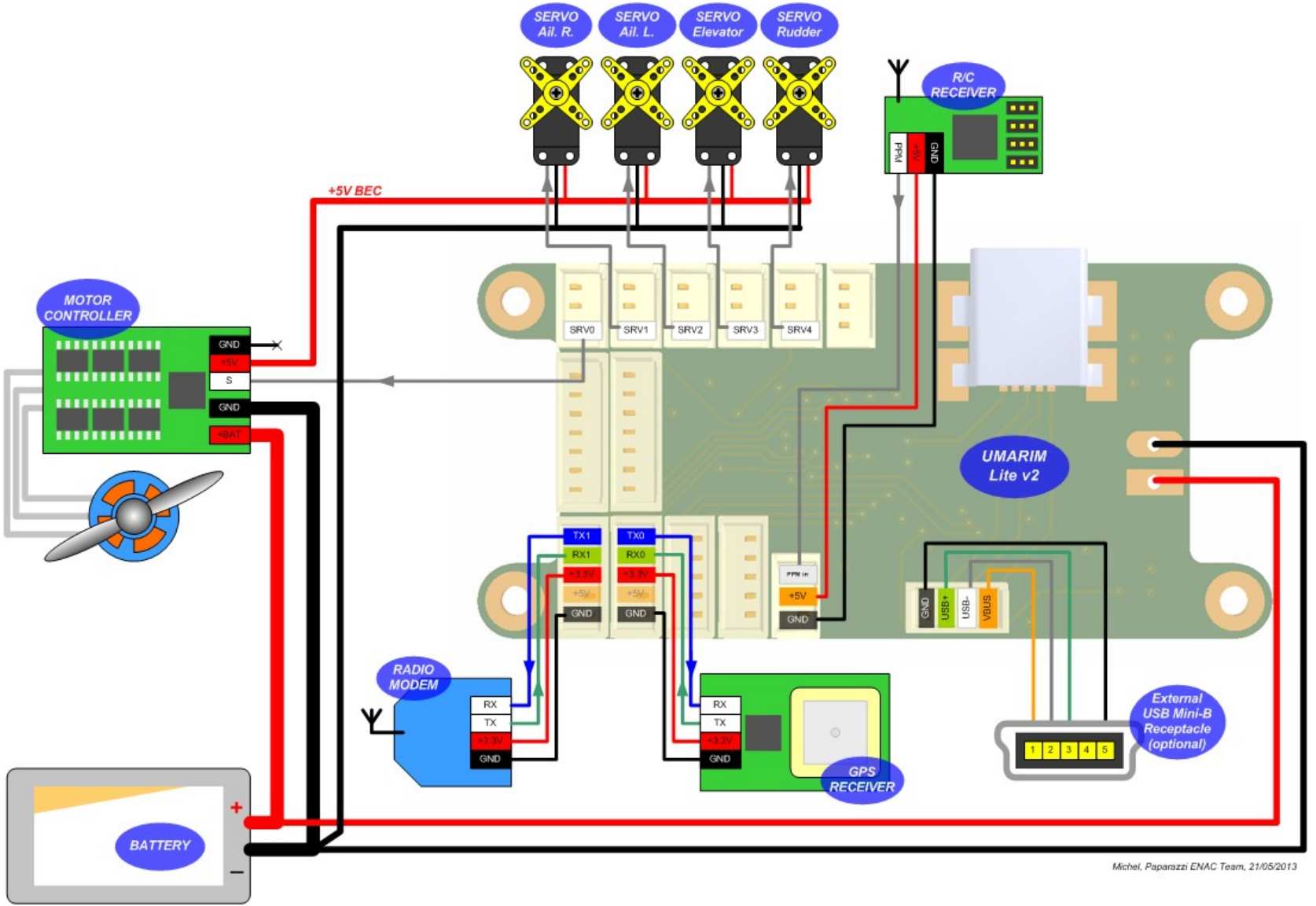
Generic System Diagram

- Fixed-wing RC aeroplane (Elevons)



Generic System Diagram

- Conventional, fixed-wing aeroplane



Generic Design

- Inputs
  - RF modem (also an output)
  - GNSS receiver (4 Hz GPS or better)
  - RC receiver(s)
  - IMU / Thermopile array
- Outputs
  - Servos, and/or
  - Speed controller(s)

Ground Checks

- Complete checklists before every flight
- Flight-management unit checks
  - Firmware; stable, up-to-date
  - Flight plan; Simulation tested
- GNSS receiver
  - GPS:HDOP, Satellites in view, RSSI, up-to-date almanac, etc
- RC link
  - control surface defelections, standard RC flight range checks
- Radio Modem
  - 2-way communication with ground control

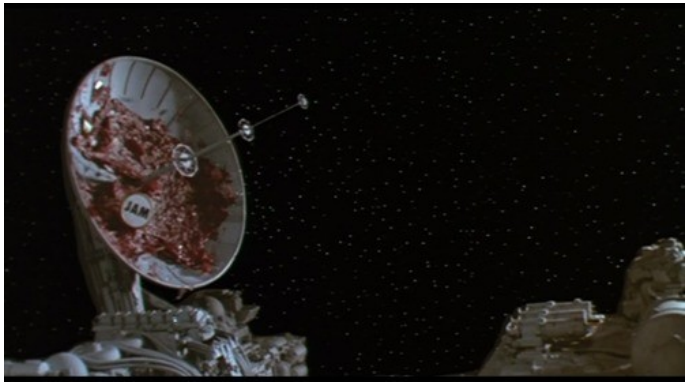
Securitah

- MILSPEC > DIY. Duh.
- Radio subject to interference, on a good day
- Kerckhoffs's principle
  - “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

Attack surface

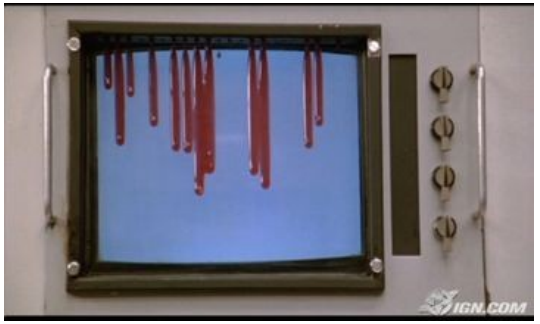
- Control systems
  - AHRS & Navigation control – relies on (take 1x out):
    - GPS
    - IMU
    - [Thermopile array]
- Control interface(s)
    - COTS/hobbyist Radio Control systems
    - 802.15 aka ZigBee FHSS radio-modems
    - Proprietary RF systems (eg; some 868MHz radio modems)
    - PLMN (data over public UMTS, GPRS, LTE, et cetera)
- Physical
  - Interdiction
  - Weaponisation not a good idea; PTSD != fun

AHRS attacks



- if (!AHRS) { exit(1); }
- Jam GPS
  - Received signal amplitude close to noise floor already
  - Dead reckoning drift becomes uncorrectable
- Magnetometer (and other components) may become unreliable with chaff or HERF
- MEMS Gyro and Accelerometer maybe harder to upset
- Autopilots may alarm-off for limp home in RPV flight mode

Jamming



- Illegal
- TL;DR
  - Easy. S/N ratio often low already
  - Buy jammers at dx.com, China websites
  - DIY with a VCO or two, mixer and amplifier
- The concept: 0 - ∞ Hz
  - Usable signal = received signal – noise floor.
  - Send broadband noise for FHSS

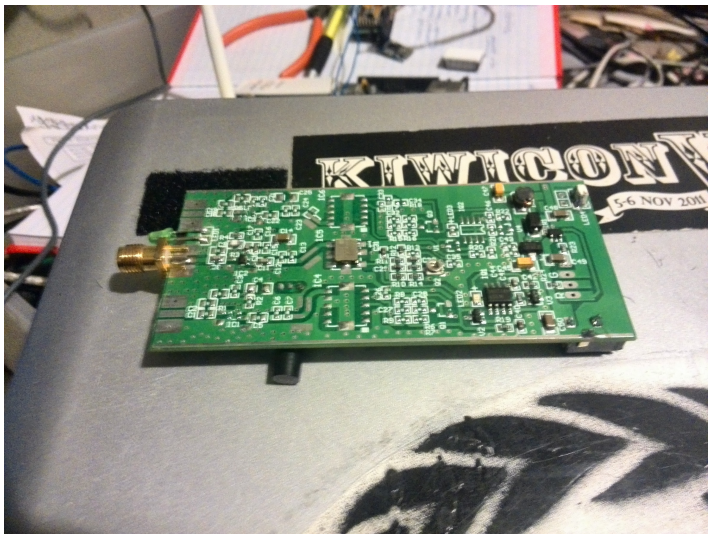
Common frequencies

- Common RC and radio-modem frequencies
  - 27 MHz
  - 29 MHz
  - 35-36 MHz
  - 40-42 MHz
  - 72 MHz
  - 433 MHz
  - 868 MHz
  - 915MHz (ISM general use)
  - 2.400-2.4835 GHz (ISM general use)

- How loss of radio control is handled varies
  - Paparazzi provides conditional flight plan blocks
  - In Ardupilot and others, an RC radio link is critical, flight plan design may afford recovery from signal loss situation (YMMV)

GPS Jamming

- Target frequencies:
  - L1: 1575.42 MHz
  - L2: 1227.60 MHz
  - (L5: 1176.45 MHz)
- Korean peninsula
  - Television often jammed
  - Radio often jammed
  - There's a market for this stuff
- Free shipping!!
- </real_security_problem>



Jamming Mitigation

- Modern GNSS receivers
- Moar power, FHSS, TDMA
- Design note: RF environment == hostile
  - Try and not rely on an RF link to complete any flight plan and land
  - Aircraft loiter / land upon unrecoverable link failure
  - RS232 can be multiplexed, piped thru crypto, old-school TTY hacked, etc
- Good antenna and placement, steering

OpenLRS

Example

- Open Sauce FHSS RC radio & modem
- Various RF chips supported, from RFM
- MAXHOPS = 24 (randomly selected from 255)
- Loop() { rfChannel++ }
- void bindRandomize() - High security
- uint32_t magic is a number I'm XOR-ing

Parrot AR Drone

Demo

- Funny story: FHSS pwns DSSS
- 2.4 GHz ISM is very polluted spectrum
- YMMV flying an AR drone:
  - Near hackers
  - Near microwaves
  - Near RC planes
  - Further than 15 meters
  - On a good day

MAVLink
(Protocol)

- Hello? Security? (difficult silence)
- Luckily 802.15 has some access controls
- Cos MAC addresses were never spoofed
-

Safety & Flight planning

- Plan your RPV and UAV flights thoroughly
- Learn about real aviation SOPs
- VFR traffic often flies low, beware of small planes
- FFS don't fly anywhere near an airport, or heliport
- Lookup CAA-published departures/approaches, routes, STARs, SIDs, ILS/DME and VORs. Understand where aircraft are, to better avoid them.
- Monitor the centre and nearest tower frequency
- Monitor ADS-B for even moar aeroplane infos