FREND

Friend Enemy Detection

1 Month = 200,000 drones deployed

1 Month = 200,000 drones deployed

2000 lost x $1000 = 2M per month

1 Month = 200,000 drones deployed

2000 lost x $1000 = 2M per month

24,000 more drones


Kinyzhak Brigade / Reuters
THE Sun

Secret Messages in Video

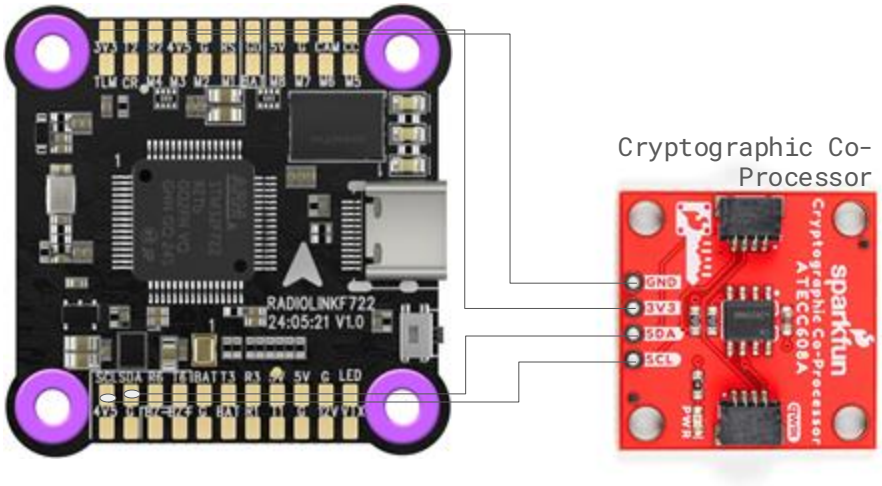

ALT 14.2m
54m
AIR
16
REDBACK
DANIEL
23 9


R E D B A C K
D A N I E L

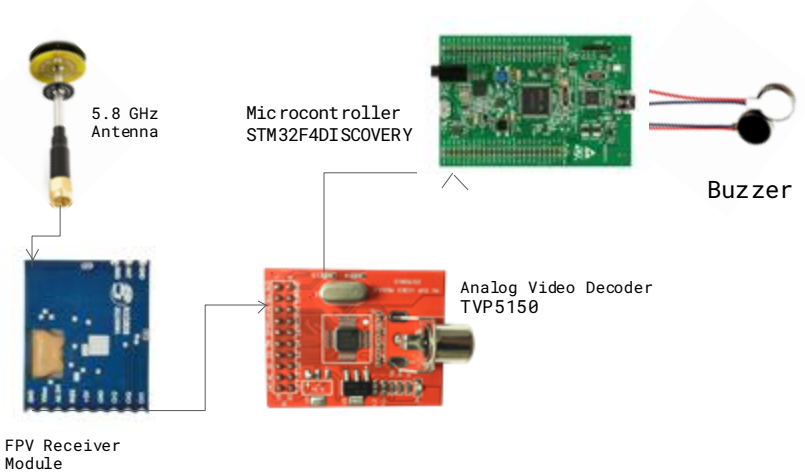

R E D B A C K
D A N I E L

SOLUTION

DRONE



RECEIVER



TEAM - FRENDZONE

Sam - Robotics

Matteo - ML

Carlo - Elec Eng

Silvio - Comp Eng

Nic – Informatics

WHAT WE NEED

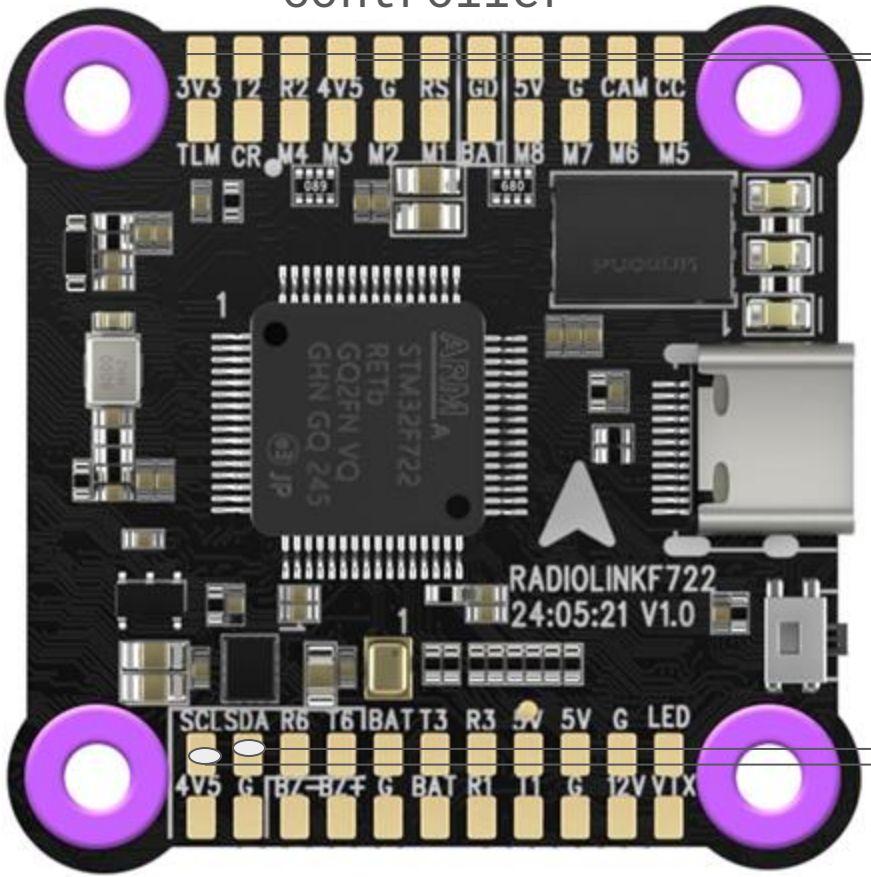
Front line contacts

Drone manufacturers

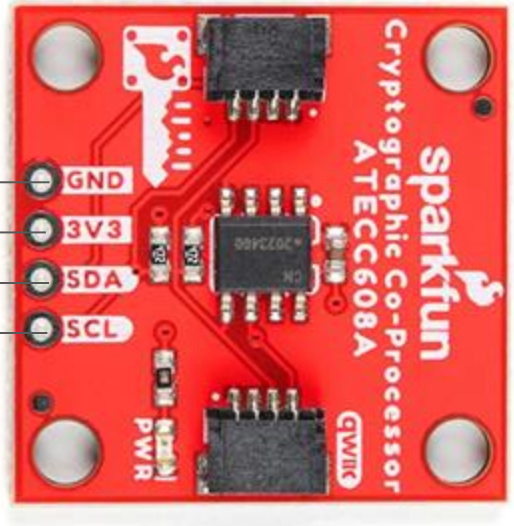
Appendix

BASIC ELECTRONIC COMPONENTS- drone

Standard Flight Controller

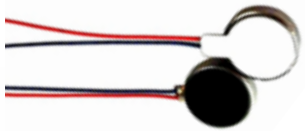


Cryptographic Co-Processor



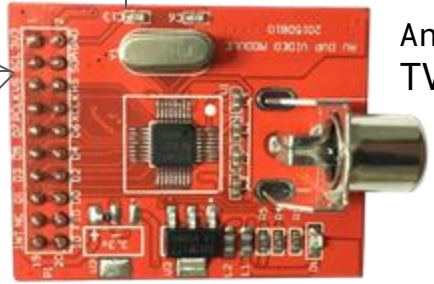
5.8 GHz
Antenna

Microcontroller
STM32F4DISCOVERY



Buzzer

FPV Receiver
Module



Analog Video Decoder
TVP5150

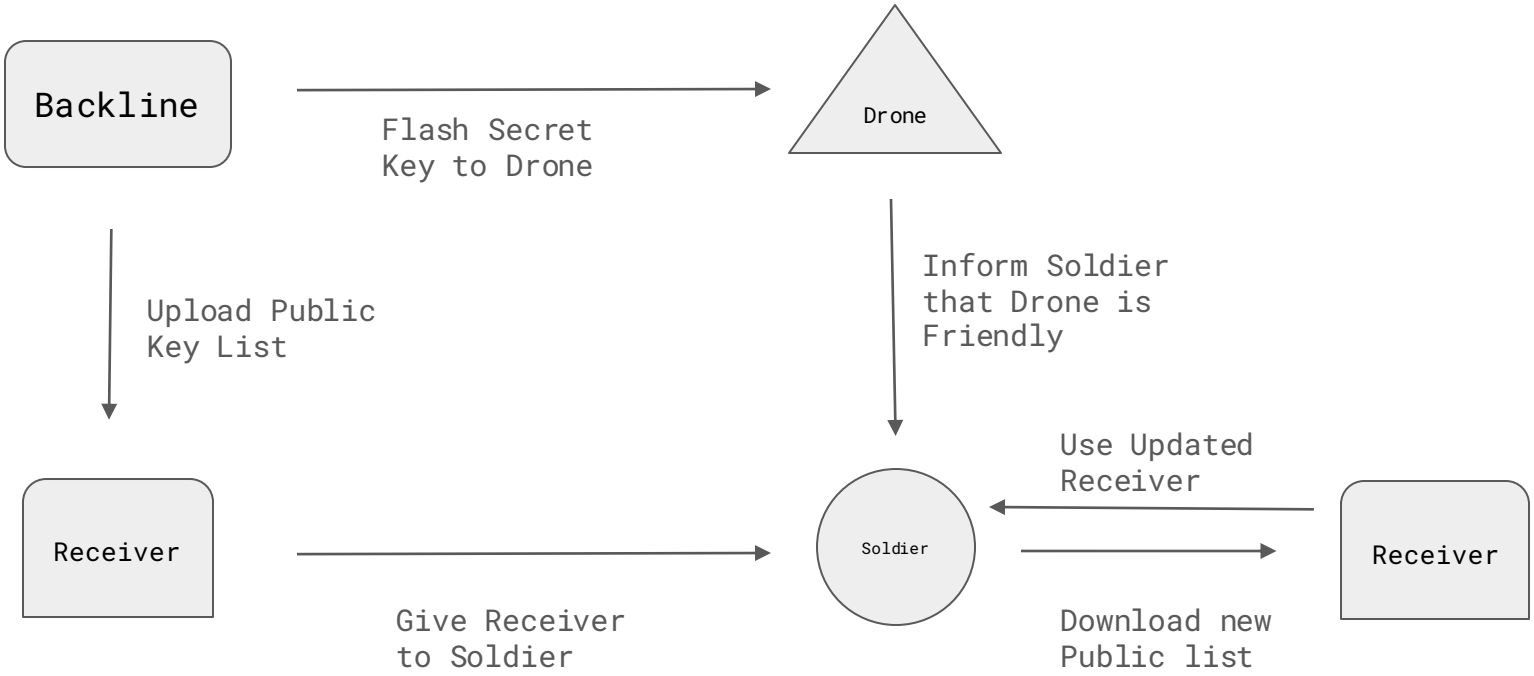
BASIC ELECTRONIC COMPONENTS- receiver

Product Roll-Out

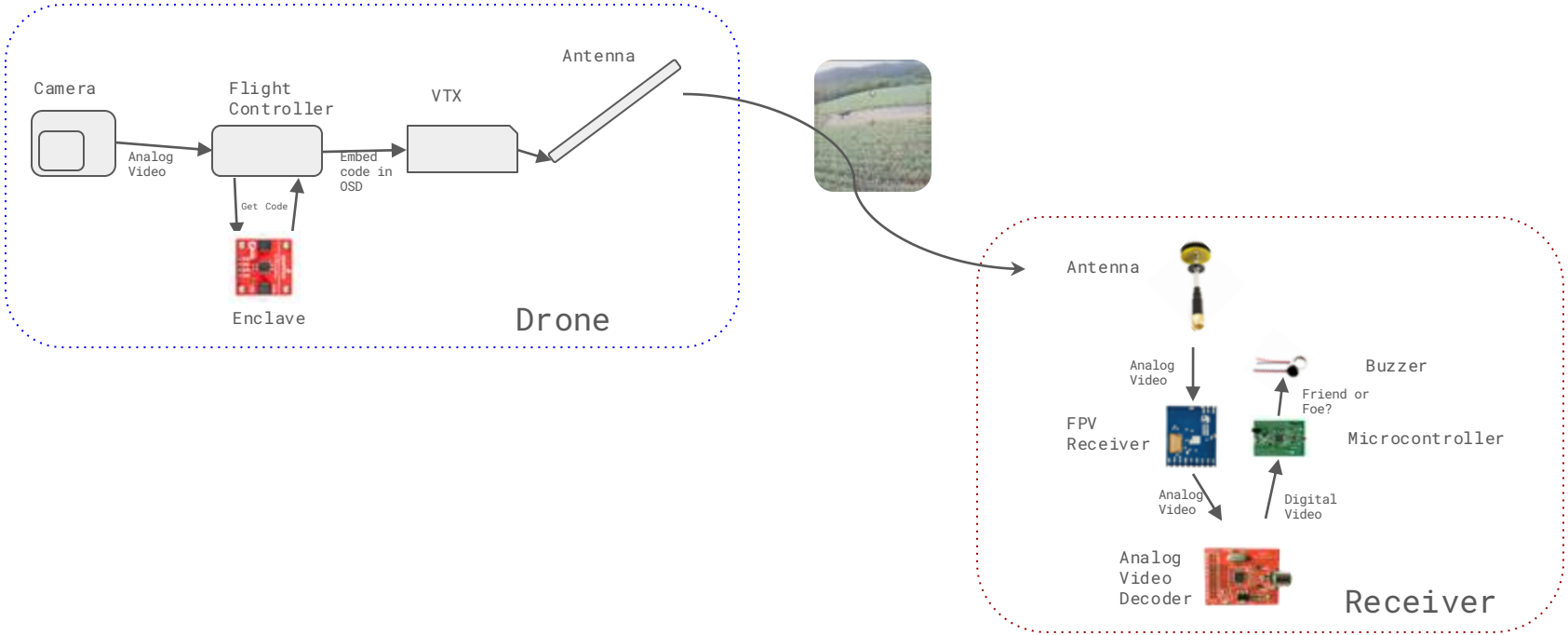
- Solder enclave on drone (manufacturer +30 sec)
- Flash extended FC software (backline +0 sec)
- Use DELTA to manage key lists

- Periodic receiver updates via DELTA managed system

Logistical Pipeline



Information Flow



Private-Public Key System

Private Key:

- Can **create codes**
- In secure enclave on drone
- Creates codes to embed into video stream

Public Key:

- Paired with a private key
- **Can validate** codes, but **cannot create** codes
- Stored in a list on receiver
- Safe to lose

THE INSPIRATION:
CHUYKA 3.0 by BLUEBIRD

Final costs

TO ADD (Drone):

6 euros (Cryptographic Co-Processor)

MAKING THE RECEIVER:

57-59 EUROS/unit (COTS price)

(Antenna 6€, Receiver 16€, Microcontroller 20€, Analog Decoder 5-7€,DFR0151 4€, other manifacturing costs 6€)

Pseudocode: how cryptography can work effectively

ENCRYPTION

Compute Encrypt(DroneID, Timestamp) with private key

Take the analog video and spot where to place the encrypted password:

Count synch pulses of analog video

place the embedded password as OSD information

DECRYPTION

(After obtaining the digital frame)

Cropping the exact patch where we know the password is hidden (we know it beforehand)

Through a threshold, decide which pixels have the right intensities for being considered as ones and zeros inside the patch

Decoding using the chosen format

Decrypt the message using the public key